Administrar VMware vSAN

Actualización 3

20 de agosto de 2019

VMware vSphere 6.7

VMware vSAN 6.7



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de Administrar VMware vSAN

En *Administrar VMware vSAN*, se describe cómo configurar y administrar un clúster de vSAN en un entorno de VMware vSphere®. En *Administrar VMware vSAN* también se explica cómo administrar los recursos de almacenamiento físico local que funcionan como dispositivos de capacidad de almacenamiento en un clúster de vSAN. De igual manera, se explica cómo definir directivas de almacenamiento para máquinas virtuales implementadas en almacenes de datos de vSAN.

Audiencia prevista

Esta información está destinada a administradores de virtualización experimentados que están familiarizados con la tecnología de virtualización, las operaciones cotidianas de los centros de datos y los conceptos de vSAN.

Para obtener más información sobre vSAN y la creación de un clúster de vSAN, consulte la guía *Planificar e implementar vSAN*.

Para obtener más información sobre cómo supervisar un clúster de vSAN y solucionar problemas, consulte la guía *Supervisar vSAN y solucionar sus problemas*.

vSphere Client y vSphere Web Client

Las instrucciones de esta guía reflejan vSphere Client (GUI basada en HTML5). También puede utilizar las instrucciones para realizar las tareas mediante vSphere Web Client (GUI basada en Flex).

Las tareas para las que el flujo de trabajo difiere significativamente entre vSphere Client y vSphere Web Client tienen procedimientos duplicados que proporcionan los pasos de acuerdo con la interfaz del cliente correspondiente. Los procedimientos que se relacionan con vSphere Web Client contienen vSphere Web Client en el título.

Nota En vSphere 6.7 Update 3, casi todas las funcionalidades de vSphere Web Client se implementan en vSphere Client. Para obtener una lista actualizada del resto de las funcionalidades no compatibles, consulte Actualizaciones de funcionalidades para vSphere Client.

Introducción a vSAN

1

VMware vSAN es una capa distribuida de software que se ejecuta de manera nativa como parte del hipervisor de ESXi. vSAN agrega dispositivos de capacidad locales o con conexión directa de un clúster de host y crea un grupo de almacenamiento individual compartido entre todos los hosts del clúster de vSAN.

vSAN admite las características de VMware que requieren almacenamiento compartido (como HA, vMotion y DRS) y, al mismo tiempo, elimina la necesidad de usar almacenamiento compartido externo y simplifica las actividades de aprovisionamiento de máquinas virtuales y configuración de almacenamiento.

Configurar y administrar un clúster de vSAN

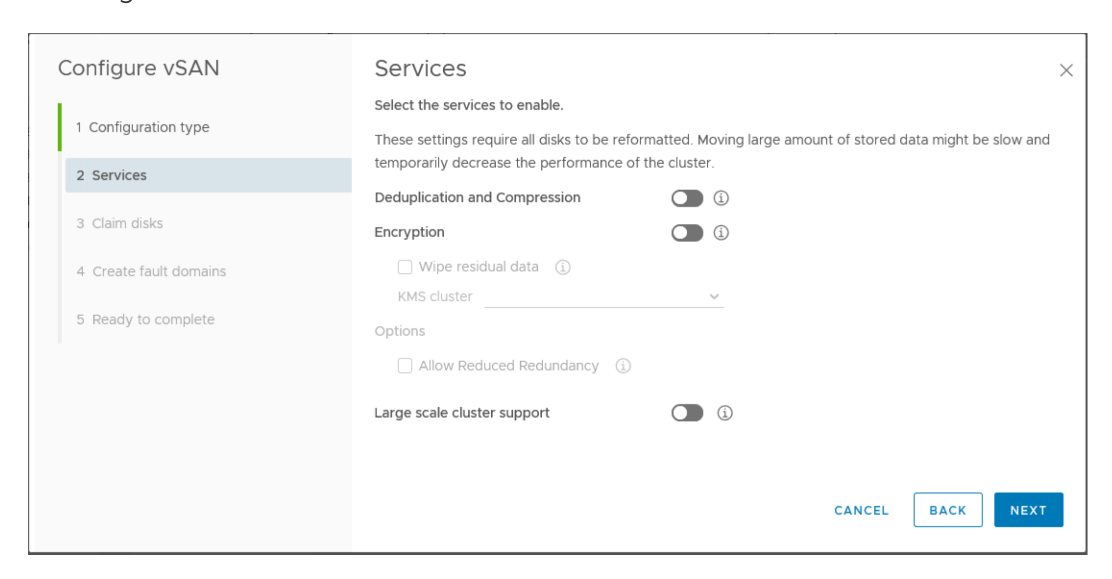
2

Puede configurar y administrar un clúster de vSAN mediante vSphere Client, los comandos esxcli y otras herramientas.

Este capítulo incluye los siguientes temas:

Configurar un clúster de vSAN mediante vSphere Client

Puede utilizar el asistente Configurar vSAN en vSphere Client basado en HTML 5 para completar la configuración básica del clúster de vSAN.



Requisitos previos

Cree un clúster y agregue hosts al clúster antes de utilizar el asistente Configurar vSAN para completar la configuración básica.

Procedimiento

1 Desplácese hasta un clúster existente en vSphere Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios** y haga clic en el botón **Configurar**.

4 Seleccione el tipo de configuración y haga clic en **Siguiente**.

   - Clúster de sitio único. Todos los hosts se encuentran en un sitio, con funciones de testigo compartidas.
   - Clúster de vSAN con dos hosts. Un host en cada sitio y un host testigo en otro sitio.
   - Clúster ampliado. Dos sitios activos, cada uno con un número par de hosts y dispositivos de almacenamiento, y un host testigo en el tercer sitio.

5 En la página **Servicios**, configure los servicios de vSAN y haga clic en **Siguiente**.

   a (Opcional) Habilite **Desduplicación y compresión** en el clúster.

   b (Opcional) Habilite **Cifrado** y seleccione un KMS.

   c (Opcional) Active la casilla **Permitir redundancia reducida** para habilitar el cifrado o la desduplicación y la compresión en un clúster de vSAN con recursos limitados. Por ejemplo, cuando el clúster tiene tres hosts con la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) establecida en 1. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

   d (Opcional) Habilite la compatibilidad con clústeres grandes para hasta 64 hosts en el clúster de vSAN.

6 En la página **Claim disks** (Reclamar discos), seleccione los discos que utilizará el clúster y haga clic en **Next** (Siguiente).

   En cada host que aporte almacenamiento, seleccione un dispositivo flash para el nivel de memoria caché y uno o más dispositivos para el nivel de capacidad.

7 Siga el asistente para completar la configuración del clúster, según el modo de tolerancia ante errores.

   a Si seleccionó **Configure two host vSAN cluster** (Configurar clúster de vSAN de dos hosts), seleccione un host testigo para el clúster y reclame los discos para el host testigo.

   b Si seleccionó **Configure stretched cluster** (Configurar clúster ampliado), defina los dominios de errores para el clúster, seleccione un host testigo y recupere los discos para el host testigo.

   c Si seleccionó **Configure fault domains** (Configurar dominios de errores), defina los dominios de errores para el clúster.

   Para obtener más información sobre los dominios de errores, consulte Administrar dominios de errores en clústeres de vSAN.

   Para obtener más información acerca de los clústeres ampliados, consulte "Introducción a los clústeres ampliados" en *Planificar e implementar vSAN*.

8 En la página **Ready to complete** (Listo para finalizar), revise la configuración y haga clic en **Finish** (Finalizar).

Resultados

Al habilitar vSAN, se crea un almacén de datos de vSAN y se registra el proveedor de almacenamiento de vSAN. Los proveedores de almacenamiento de vSAN son componentes de software integrados que comunican las funcionalidades de almacenamiento del almacén de datos a vCenter Server.

Pasos siguientes

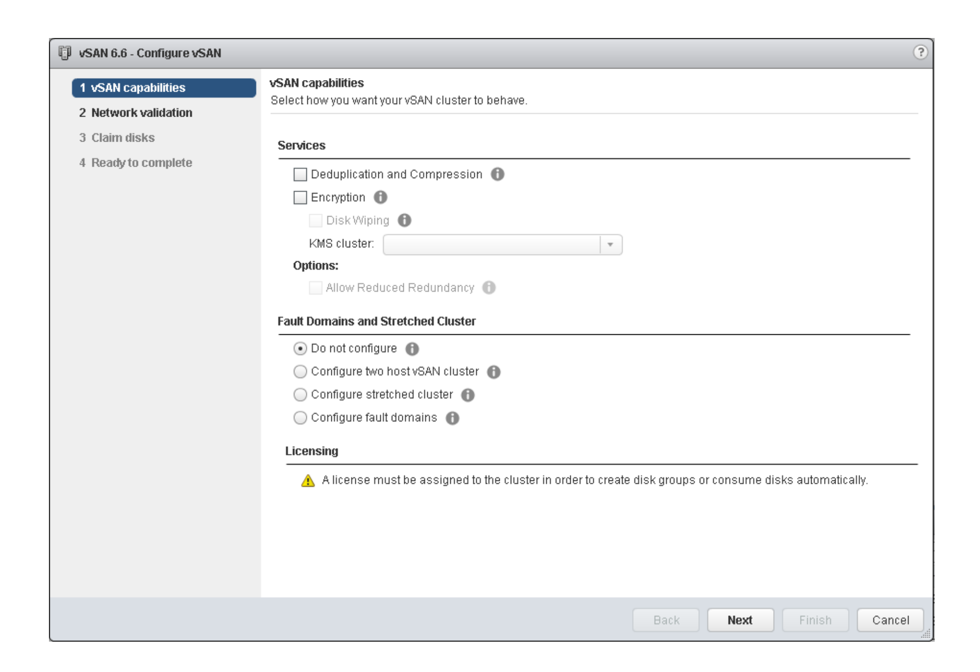
Compruebe que se haya creado el almacén de datos de vSAN. Consulte Ver el almacén de datos de vSAN.

Compruebe que el proveedor de almacenamiento de vSAN esté registrado. Consulte Ver los proveedores de almacenamiento de vSAN.

Puede reclamar los dispositivos de almacenamiento o crear grupos de discos. Consulte *Administrar VMware vSAN*.

Configurar un clúster para vSAN mediante vSphere Web Client

Puede utilizar el asistente Configurar vSAN para completar la configuración básica del clúster de vSAN.



Requisitos previos

Debe configurar un clúster y agregar hosts al clúster antes de utilizar el asistente Configurar vSAN para completar la configuración básica.

Procedimiento

1 Desplácese hasta un clúster existente en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General** y haga clic en el botón **Configure** (Configurar).

4 Seleccione **vSAN capabilities** (Funcionalidades de vSAN).

   a (Opcional) Active la casilla **Deduplication and Compression** (Desduplicación y compresión) si desea habilitar la desduplicación y compresión en el clúster.

      Puede activar la casilla **Permitir redundancia reducida** para habilitar la desduplicación y la compresión en un clúster de vSAN con recursos limitados, como un clúster de tres hosts en la que la opción **Nivel primario de errores que se toleran** se establece en 1. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

   b (Opcional) Active la casilla **Encryption** (Cifrado) si desea habilitar el cifrado de datos en reposo y seleccione un KMS.

c Seleccione el modo de tolerancia ante errores del clúster.

Opción	Descripción
Do not configure (No configurar)	Configuración predeterminada utilizada para un clúster de vSAN de un solo sitio.
Clúster de vSAN con dos hosts	Proporciona tolerancia ante errores para un clúster que tiene dos hosts en la oficina remota, con un host testigo en la oficina principal. Establezca la directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1.
Clúster ampliado	Admite dos sitios activos, incluso con un número par de hosts y dispositivos de almacenamiento, y un host testigo en el tercer sitio.
Configure fault domains (Configurar dominios de errores)	Admite dominios de errores que puede utilizar para agrupar hosts de vSAN que podrían fallar en conjunto. Asigne uno o más hosts a cada dominio de errores.

d Puede activar la casilla **Permitir redundancia reducida** para habilitar el cifrado o la desduplicación y la compresión en un clúster de vSAN con recursos limitados. Por ejemplo, cuando el clúster tiene tres hosts con la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) establecida en 1. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

5 Haga clic en **Next** (Siguiente).

6 En la página **Validación de red** compruebe la configuración para los adaptadores de VMkernel de vSAN y haga clic en **Siguiente**.

7 En la página **Claim disks** (Reclamar discos), seleccione los discos que utilizará el clúster y haga clic en **Next** (Siguiente).

En cada host que aporte almacenamiento, seleccione un dispositivo flash para el nivel de memoria caché y uno o más dispositivos para el nivel de capacidad.

8 Siga el asistente para completar la configuración del clúster, según el modo de tolerancia ante errores.

a Si seleccionó **Configure two host vSAN cluster** (Configurar clúster de vSAN de dos hosts), seleccione un host testigo para el clúster y reclame los discos para el host testigo.

b Si seleccionó **Configure stretched cluster** (Configurar clúster ampliado), defina los dominios de errores para el clúster, seleccione un host testigo y recupere los discos para el host testigo.

c Si seleccionó **Configure fault domains** (Configurar dominios de errores), defina los dominios de errores para el clúster.

Para obtener más información sobre los dominios de error de clústeres ampliados, consulte *Administrar VMware vSAN*.

9 En la página **Ready to complete** (Listo para finalizar), revise la configuración y haga clic en **Finish** (Finalizar).

Habilitar vSAN en un clúster existente

Puede editar las propiedades de un clúster a fin de habilitar vSAN para un clúster existente.

Requisitos previos

Compruebe que el entorno cumpla con todos los requisitos. Consulte "Requisitos para habilitar vSAN" en *Administrar VMware vSAN*.

Procedimiento

1 Desplácese hasta un clúster de host.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios**. b (Opcional) Habilite la desduplicación y la compresión en el clúster. vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster. c (Opcional) Habilite el cifrado en el clúster y seleccione un servidor KMS. vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster. d (Opcional) Seleccione Permitir redundancia reducida. Si es necesario, vSAN reducirá el nivel de protección de las máquinas virtuales, mientras se habilitan la desduplicación y la compresión o el cifrado.
vSphere Web Client	a En vSAN, seleccione **General**. b En el panel vSAN está activado, haga clic en el botón **Editar**. c (Opcional) Si desea habilitar la desduplicación y compresión en el clúster, marque la casilla **Deduplication and compression** (Desduplicación y compresión). vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster. d (Opcional) Si desea habilitar el cifrado en el clúster, marque la casilla **Encryption** (Cifrado) y seleccione un servidor KMS. vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster.

3 Haga clic en **Aceptar** o en **Aplicar** para confirmar su selección.

Pasos siguientes

Puede reclamar los dispositivos de almacenamiento o crear grupos de discos. Consulte *Administrar VMware vSAN*.

Deshabilitar vSAN

Puede desactivar vSAN para un clúster de host.

Cuando se deshabilita el clúster de vSAN, todas las máquinas virtuales ubicadas en el almacén de datos compartido de vSAN dejan de estar accesibles. Si va a usar la máquina virtual mientras vSAN está deshabilitado, asegúrese de migrar las máquinas virtuales del almacén de datos de vSAN a otro almacén de datos antes de deshabilitar el clúster de vSAN.

Requisitos previos

Compruebe que los hosts estén en modo de mantenimiento.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios**. b Haga clic en **Desactivar vSAN**. c En el cuadro de diálogo Desactivar vSAN, confirme la selección.
vSphere Web Client	a En vSAN, seleccione **General**. b En el panel vSAN está activado, haga clic en el botón **Editar**. c Desactive la casilla **Turn On** (Activar) de vSAN.

Editar la configuración de vSAN

Puede editar la configuración del clúster de vSAN para cambiar el método para reclamar discos y para habilitar la desduplicación y la compresión.

Edite la configuración de un clúster de vSAN existente si desea habilitar la desduplicación y la compresión, o para cambiar el método de cifrado. Si habilita la desduplicación y la compresión, o el cifrado, el formato en disco del clúster se actualiza automáticamente a la versión más reciente.

Procedimiento

1 Desplácese hasta el clúster de hosts de vSAN.

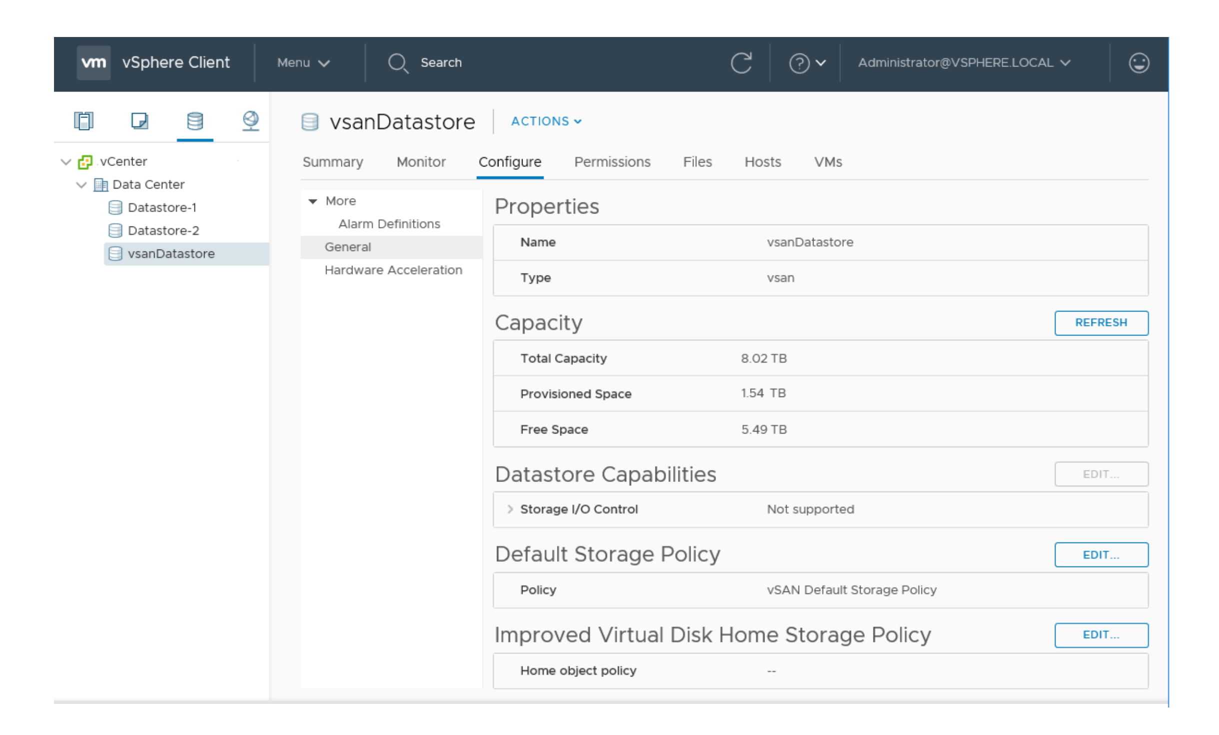
2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios**. b Haga clic en el botón **Editar** correspondiente al servicio que desea configurar. ■ Habilite o deshabilite la desduplicación y la compresión. ■ Configure el cifrado de vSAN. ■ Configure el servicio de rendimiento de vSAN. ■ Configure el servicio del destino iSCSI. ■ Configure las opciones avanzadas: ■ Temporizador de reparación de objetos ■ Ubicación de lectura de sitios para clústeres ampliados ■ Aprovisionamiento de intercambio fino ■ Compatibilidad con clústeres grandes para hasta 64 hosts ■ Redistribución automática c Modifique la configuración para que coincida con sus requisitos.
vSphere Web Client	a En vSAN, seleccione **General**. b En el panel vSAN está activado, haga clic en el botón **Editar**. c (Opcional) Si desea habilitar la desduplicación y compresión en el clúster, marque la casilla **Deduplication and compression** (Desduplicación y compresión). vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster. d (Opcional) Si desea habilitar el cifrado en el clúster, marque la casilla **Encryption** (Cifrado) y seleccione un servidor KMS. vSAN actualizará automáticamente el formato en disco, lo que provocará un reformateo sucesivo de cada grupo de discos del clúster.

3 Haga clic en **Aceptar** o en **Aplicar** para confirmar su selección.

Ver el almacén de datos de vSAN

Después de activar vSAN, se crea un solo almacén de datos. Puede revisar la capacidad del almacén de datos de vSAN.



Requisitos previos

Active vSAN y configure los grupos de discos.

Procedimiento

1. Desplácese hasta el almacenamiento.
2. Seleccione el almacén de datos de vSAN.
3. Haga clic en la pestaña **Configurar**.
4. Revise la capacidad del almacén de datos de vSAN.

   El tamaño del almacén de datos de vSAN depende de la cantidad de dispositivos de capacidad por cada host ESXi de la cantidad de hosts ESXi en el clúster. Por ejemplo, si un host cuenta con 7 dispositivos de capacidad de 2 TB y el clúster incluye 8 hosts, la capacidad de almacenamiento aproximada es la siguiente: 7 x 2 TB x 8 = 112 TB. Al usar la configuración basada íntegramente en tecnología flash, se utilizan dispositivos flash para la capacidad. Para las configuraciones híbridas, se utilizan discos magnéticos para la capacidad.

   Algo de capacidad se asigna para los metadatos.

   - El formato en disco versión 1.0 agrega aproximadamente 1 GB por dispositivo de capacidad.
   - El formato en disco versión 2.0 agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo.

- El formato en disco versión 3.0 y posteriores agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo. La desduplicación y la compresión con la suma de comprobación de software habilitada requieren una sobrecarga adicional de aproximadamente 6,2 % de capacidad por dispositivo.

Pasos siguientes

Cree una directiva de almacenamiento para máquinas virtuales con las capacidades de almacenamiento del almacén de datos de vSAN. Para obtener información, consulte el documento *Almacenamiento de vSphere*.

Cargar archivos o carpetas en almacenes de datos de vSAN

Puede cargar archivos NFS, VMFS y VMDK en un almacén de datos de vSAN. También puede cargar carpetas en un almacén de datos de vSAN. Para obtener más información sobre los almacenes de datos, consulte *Almacenamiento de vSphere*.

Para la carga de un archivo VMDK en un almacén de datos de vSAN, rigen las siguientes consideraciones:

- Solo puede cargar archivos VMDK optimizados para transmisión en un almacén de datos de vSAN. El formato de archivo optimizado para secuencias de VMware es un formato monolítico disperso comprimido para la transmisión por secuencias. Si el archivo VMDK no está en formato optimizado para transmisión, antes de cargarlo, conviértalo a dicho formato mediante la utilidad vmware-vdiskmanager command-line. Para obtener más información, consulte la *Guía de usuario del administrador de disco virtual*.
- Cuando se carga un archivo VMDK en un almacén de datos de vSAN, el archivo hereda la directiva predeterminada de ese almacén de datos. Por lo tanto, el archivo VMDK no hereda la directiva de la máquina virtual desde la que se descargó. vSAN crea los objetos aplicando la directiva predeterminada vsanDatastore, que es RAID-1. Puede cambiar la directiva predeterminada del almacén de datos. Consulte Cambiar la directiva de almacenamiento predeterminada de los almacenes de datos de vSAN .
- El archivo VMDK debe cargarse en la carpeta de inicio de la máquina virtual.

Procedimiento

1 Desplácese al almacén de datos de vSAN.

2 Haga clic en la pestaña **Archivos**.

Opción	Descripción
Cargar archivos	a Seleccione la carpeta de destino y haga clic en **Cargar archivos**. Verá un mensaje donde se le informa de que solo puede cargar archivos VMDK en el formato optimizado para transmisión de VMware. Si intenta cargar un archivo VMDK en un formato diferente, verá un mensaje de error interno del servidor. b Haga clic en **Cargar**. c Busque el elemento que desea cargar en el equipo local y haga clic en **Abrir**.
Cargar carpetas	a Seleccione la carpeta de destino y haga clic en **Cargar carpeta**. Verá un mensaje donde se le informa de que solo puede cargar archivos VMDK en el formato optimizado para transmisión de VMware. b Haga clic en **Cargar**. c Busque el elemento que desea cargar en el equipo local y haga clic en **Abrir**.

Descargar archivos o carpetas de almacenes de datos de vSAN

Puede descargar archivos y carpetas de un almacén de datos de vSAN. Para obtener más información sobre los almacenes de datos, consulte *Almacenamiento de vSphere*.

Los archivos vmdk se descargan como archivos optimizados para secuencias con el nombre de archivo `<vmdkName>_stream.vmdk`. El formato de archivo optimizado para secuencias de VMware es un formato monolítico disperso comprimido para la transmisión por secuencias.

Puede convertir un archivo vmdk optimizado para secuencias de VMware a otros formatos de archivo vmdk mediante la utilidad de línea de comandos vmware-vdiskmanager. Para obtener más información, consulte la *Guía de usuario del administrador de disco virtual*.

Procedimiento

1 Desplácese al almacén de datos de vSAN.

2 Haga clic en la pestaña **Archivos** y, a continuación, en **Descargar**.

  Verá un mensaje donde se advierte que los archivos vmdk se descargarán de los almacenes de datos de vSAN en el formato optimizado para secuencias de VMware con la extensión de nombre de archivo `.stream.vmdk`.

3 Haga clic en **Descargar**.

4 Busque el elemento que desea descargar y, a continuación, haga clic en **Descargar**.

Usar las directivas de vSAN

3

Al usar vSAN, puede definir requisitos de almacenamiento de máquinas virtuales, como el rendimiento y la disponibilidad, mediante una directiva. vSAN garantiza que a cada máquina virtual implementada en los almacenes de datos de vSAN se le asigne, al menos, una directiva de almacenamiento.

Una vez asignados, los requisitos de la directiva de almacenamiento se traspasan a la capa de vSAN cuando se crea una máquina virtual. El dispositivo virtual se distribuye en el almacén de datos de vSAN para cumplir con los requisitos de rendimiento y disponibilidad.

vSAN utiliza proveedores de almacenamiento para suministrar información sobre el almacenamiento subyacente a vCenter Server. Esta información ayuda a tomar las decisiones adecuadas sobre la selección de máquinas virtuales y a supervisar el entorno de almacenamiento.

Este capítulo incluye los siguientes temas:

Acerca de las directivas de vSAN

Las directivas de almacenamiento de vSAN definen los requisitos de almacenamiento para las máquinas virtuales. Estas directivas determinan cómo los objetos de almacenamiento de máquinas virtuales se aprovisionan y asignan dentro del almacén de datos para garantizar el nivel de servicio requerido.

Al habilitar vSAN en un clúster del host, se crea un solo almacén de datos de vSAN y, asimismo, se asigna una directiva de almacenamiento predeterminada al almacén de datos.

Cuando se conocen los requisitos de almacenamiento de las máquinas virtuales, es posible crear una directiva de almacenamiento que hace referencia a las funcionalidades que anuncia el almacén de datos. Puede crear varias directivas para capturar distintos tipos o distintas clases de requisitos.

Se asigna a cada máquina virtual implementada en los almacenes de datos de vSAN al menos una directiva de almacenamiento de máquinas virtuales. Puede asignar estas directivas de almacenamiento al crear o editar máquinas virtuales.

Nota Si no asigna una directiva de almacenamiento a una máquina virtual, vSAN asigna una directiva predeterminada. La directiva predeterminada tiene la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) configurada en 1, una sola fracción de disco por objeto y un disco virtual con aprovisionamiento fino.

El objeto de intercambio de máquina virtual y el objeto de memoria de instantáneas de máquina virtual no cumplen con las directivas de almacenamiento asignadas a una máquina virtual. Estos objetos se configuran con la opción **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Es posible que la disponibilidad de estos objetos no sea igual a la de otros objetos que tengan asignada una directiva con un valor diferente para **Primary level of failures to tolerate** (Nivel principal de errores que se toleran).

Tabla 3-1. Reglas de la directiva de almacenamiento

Funcionalidad	Descripción
Nivel primario de errores que se toleran (Primary level of failures to tolerate, PFTT)	Define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de una máquina virtual. Para errores `n` tolerados, cada dato escrito se almacena en las ubicaciones `n+1`, incluidas las copias de paridad si se utiliza RAID 5 o RAID 6. Al aprovisionar una máquina virtual, si no se selecciona una directiva de almacenamiento, vSAN asigna esta directiva como la directiva de almacenamiento de máquina virtual predeterminada. Si se configuran dominios de errores, se requieren `2n+1` dominios de errores con hosts que aporten capacidad. Un host que no forma parte de ningún dominio de errores se considera su propio dominio de errores de host individual. El valor predeterminado es 1. El valor máximo es 3. **Nota** Si no desea que vSAN proteja una sola copia reflejada de objetos de máquina virtual, puede especificar el valor de **PFTT** como 0. Sin embargo, es posible que el host experimente demoras inusuales al entrar en el modo de mantenimiento. Los retrasos ocurren porque vSAN debe evacuar el objeto del host para que la operación de mantenimiento se complete correctamente. Si se establece el valor de **PFTT** como 0, los datos quedan desprotegidos y estos se pueden perder cuando el clúster de vSAN detecta un error de dispositivo. **Nota** Si se crea una directiva de almacenamiento y no se especifica un valor para **PFTT**, vSAN crea una sola copia reflejada de los objetos de máquina virtual. Puede tolerar un solo error. Sin embargo, si ocurren varios errores de componentes, los datos podrían estar en riesgo. En un clúster ampliado, esta regla define el número de errores de sitios que puede tolerar un objeto de máquina virtual. Puede utilizar **PFTT** con **SFTT** para proporcionar protección contra errores locales para los objetos en los sitios de datos. El valor máximo de un clúster ampliado es 1.
Nivel secundario de errores que se toleran (Secondary level of failures to tolerate, SFTT)	En un clúster ampliado, esta regla define el número de errores de host adicionales que puede tolerar el objeto después de alcanzar el número de errores de sitios definido por **PFTT**. Si **PFTT** es igual a 1 y **SFTT** es igual a 2, y un sitio no está disponible, el clúster puede tolerar dos errores de host adicionales. El valor predeterminado es 1. El valor máximo es 3.
Localidad de datos	En un clúster ampliado, esta regla solo se encuentra disponible si el atributo **Primary level of failures to tolerate** (Nivel primario de errores que se toleran) se configura en 0. Puede configurar la regla **Localidad de datos** como **Ninguno**, **Preferido** o **Secundario**. Esta regla permite limitar los objetos de máquina virtual a un sitio o un host seleccionados en el clúster ampliado. El valor predeterminado es None (Ninguno).

Tabla 3-1. Reglas de la directiva de almacenamiento (continuación)

Funcionalidad	Descripción
Failure tolerance method (Método de tolerancia ante errores)	Especifica si el método de replicación de datos optimiza el rendimiento o la capacidad. Si selecciona **RAID-1 (reflejo): rendimiento**, vSAN utiliza más espacio de disco para colocar los componentes de los objetos, pero proporciona un mejor rendimiento para acceder a los objetos. Si selecciona **RAID-5/6 (codificación de borrado): capacidad**, vSAN utiliza menos espacio de disco, pero se reduce el rendimiento. Puede utilizar RAID 5 aplicando el atributo **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) a los clústeres con cuatro o más dominios de errores y establecer **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Puede utilizar RAID 6 aplicando el atributo **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) a los clústeres con seis o más dominios de errores y establecer **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 2. En los clústeres ampliados con la opción **Nivel secundario de errores que se toleran** configurada, esta regla solo se aplica a **Nivel secundario de errores que se toleran**. Para obtener más información sobre RAID 5 o RAID 6, consulte Usar la codificación de borrado RAID 5 o RAID 6 .
Number of disk stripes per object (Número de fracciones de disco por objeto)	El número mínimo de dispositivos de capacidad entre los que se fracciona cada réplica de un objeto de una máquina virtual. Un valor mayor que 1 produce un mejor rendimiento, pero también un mayor uso de los recursos del sistema. El valor predeterminado es 1 y el máximo es 12. No cambie el valor de fraccionamiento predeterminado. En un entorno híbrido, las fracciones de discos se distribuyen entre discos magnéticos. Para una configuración basada en flash, el fraccionamiento se realiza entre los dispositivos flash que conforman la capa de capacidad. Asegúrese de que el entorno de vSAN tenga suficientes dispositivos de capacidad presentes para adecuarse a la solicitud.

Tabla 3-1. Reglas de la directiva de almacenamiento (continuación)

Funcionalidad	Descripción
Flash read cache reservation (Reserva de Flash Read Cache)	La capacidad flash reservada como memoria caché de lectura para el objeto de la máquina virtual. Se especifica como un porcentaje del tamaño lógico del objeto del disco de la máquina virtual (vmdk). La capacidad flash reservada no puede ser utilizada por otros objetos. La capacidad flash no reservada se comparte de manera equitativa entre todos los objetos. Utilice esta opción solamente para solucionar problemas de rendimiento específicos. No es necesario establecer una reserva para obtener memoria caché. La configuración de las reservas de memoria caché de lectura podría ocasionar problemas cuando se transfiere el objeto de la máquina virtual, debido a que los ajustes de reserva de la memoria caché siempre se incluyen con el objeto. El atributo de la directiva de almacenamiento de reserva de Flash Read Cache solo es compatible con las configuraciones híbridas. No se debe usar este atributo al definir una directiva de almacenamiento de máquina virtual para un clúster basado íntegramente en tecnología flash. El valor predeterminado es 0 %. El valor máximo es 100 %. **Nota** Como opción predeterminada, vSAN asigna memoria caché de lectura de manera dinámica a los objetos de almacenamiento en función de la demanda. Esta característica representa el uso más flexible y más óptimo de los recursos. Como consecuencia, por lo general, no es necesario cambiar el valor predeterminado de 0 para este parámetro. Si desea aumentar el valor en el momento de solucionar un problema de rendimiento, sea cuidadoso. El sobreaprovisionamiento de reservas de memoria caché entre varias máquinas virtuales puede implicar un desperdicio de espacio en el dispositivo flash por reservas excesivas. Estas reservas de memoria caché no se pueden usar para atender las cargas de trabajo para las que se necesita espacio en cierto momento. Este desperdicio de espacio y falta de disponibilidad podrían causar una degradación en el rendimiento.
Force provisioning (Forzar aprovisionamiento)	Si la opción se establece en **Yes** (Sí), el objeto se aprovisiona incluso cuando el almacén de datos no puede satisfacer las directivas **Primary level of failures to tolerate** (Nivel principal de errores que se toleran), **Number of disk stripes per object** (Número de fracciones de disco por objeto) y **Flash read cache reservation** (Reserva de Flash Read Cache) especificadas en la directiva de almacenamiento. Use este parámetro en escenarios de arranque y durante una interrupción cuando el aprovisionamiento estándar ya no sea posible. El valor predeterminado **No** es aceptable para la mayoría de los entornos de producción. vSAN no aprovisiona una máquina virtual cuando no se cumplen los requisitos de la directiva; sin embargo, crea correctamente la directiva de almacenamiento definida por el usuario.

Tabla 3-1. Reglas de la directiva de almacenamiento (continuación)

Funcionalidad	Descripción
Reserva de espacio de objetos	Porcentaje del tamaño lógico del objeto de disco de máquina virtual (vmdk) que se debe reservar o al que se debe aplicar aprovisionamiento grueso al implementar las máquinas virtuales. Se encuentran disponibles las siguientes opciones: ■ Aprovisionamiento fino (predeterminado) ■ 25 % de reserva ■ 50 % de reserva ■ 75 % de reserva ■ Aprovisionamiento grueso
Disable object checksum (Deshabilitar suma de comprobación de objetos)	Si la opción se establece en **No**, el objeto calcula la información de suma de comprobación para garantizar la integridad de sus datos. Si esta opción se establece en **Yes** (Sí), el objeto no calcula la información de suma de comprobación. vSAN utiliza la suma de comprobación de extremo a extremo para garantizar la integridad de los datos confirmando que cada copia de un archivo sea exactamente igual que el archivo de origen. El sistema comprueba la validez de los datos durante las operaciones de lectura/escritura y, si se detecta un error, vSAN repara los datos o informa del error. Si se detecta una discrepancia en la suma de comprobación, vSAN repara automáticamente los datos sobrescribiendo los datos incorrectos con los datos correctos. Se realiza el cálculo de la suma de comprobación y la corrección de errores como operaciones en segundo plano. La configuración predeterminada para todos los objetos del clúster es **No**, lo que significa que la suma de comprobación está habilitada.
IOPS limit for object (Límite de IOPS para objeto)	Define el límite de IOPS para un objeto, como VMDK. El valor de IOPS se calcula como el número de operaciones de E/S, utilizando un tamaño ponderado. Si el sistema utiliza el tamaño de base predeterminado de 32 KB, una E/S de 64 KB representa dos operaciones de E/S. Al calcular las IOPS, la lectura y escritura se consideran equivalentes, pero no se consideran la proporción de aciertos de la memoria caché ni la secuencialidad. Si las IOPS de un disco exceden el límite, se aceleran las operaciones de E/S. Si **IOPS limit for object** (Límite de IOPS para objeto) se establece en 0, no se aplicarán los límites de IOPS. vSAN permite que el objeto duplique la tasa del límite de E/S por segundo durante el primer segundo de la operación o después de un período de inactividad.

Al trabajar con directivas de almacenamiento de máquinas virtuales, debe comprender la manera en que las funcionalidades de almacenamiento afectan al consumo de la capacidad de almacenamiento en el clúster de vSAN. Para obtener más información sobre las consideraciones de diseño y definición de tamaño de las directivas de almacenamiento, consulte "Diseñar un clúster de vSAN y definir su tamaño" en *Administrar VMware vSAN*.

Cómo administra vSAN los cambios de directivas

vSAN 6.7 Update 3 y las versiones posteriores administran los cambios de directivas para reducir la cantidad de espacio transitorio que se consume en todo el clúster. La capacidad transitoria se genera cuando vSAN vuelve a configurar objetos para un cambio de directiva.

Cuando se modifica una directiva, el cambio se acepta, pero no se aplica de inmediato. vSAN procesa por lotes las solicitudes de cambios de directivas y las ejecuta de forma asíncrona para mantener una cantidad fija de espacio transitorio.

Los cambios de directivas se rechazan inmediatamente si los motivos no se relacionan con la capacidad, como el cambio de una directiva de RAID5 a RAID6 en un clúster de cinco nodos.

Es posible ver el uso de capacidad transitoria en el monitor de capacidad de vSAN. Para comprobar el estado de un cambio de directiva en un objeto, use el servicio de estado de vSAN para comprobar el estado del objeto vSAN.

Afinidad de host

La directiva de almacenamiento de afinidad de host de vSAN permite almacenar una sola copia de los datos en el host local de una máquina virtual.

La directiva de almacenamiento de afinidad de host de vSAN adapta la eficacia y la resistencia de vSAN a aplicaciones de última generación que no comparten nada. Cuando se utiliza esta directiva, vSAN mantiene una sola copia de los datos, la cual se almacena en el host local que ejecuta la máquina virtual. Esta directiva se ofrece como una opción de implementación de macrodatos (Hadoop, Spark), NoSQL y otras aplicaciones de este tipo que mantienen la redundancia de datos en la capa de aplicación.

La afinidad de host de vSAN presenta requisitos y directrices específicos que requieren la validación de VMware para garantizar una implementación correcta. La directiva de afinidad de host de vSAN debe aplicarse a todas las máquinas virtuales del clúster y no puede combinarse con otras directivas en el mismo clúster. El cifrado y la desduplicación de vSAN no se pueden usar con la directiva de afinidad de host de vSAN. Las opciones vSphere DRS y HA deben desactivarse para evitar el movimiento automatizado de máquinas virtuales.

Los administradores interesados en esta función deben ponerse en contacto con VMware para enviar una solicitud de intención de implementación. VMware evaluará la solicitud para asegurarse de que la implementación cumple los requisitos antes de aprobarla para su uso en la producción y el soporte. VMware no admitirá ninguna implementación que carezca de aprobación explícita. Para obtener más información, póngase en contacto con su representante de VMware.

Ver los proveedores de almacenamiento de vSAN

Al habilitar vSAN, automáticamente se configura y se registra un proveedor de almacenamiento para cada host del clúster de vSAN.

Los proveedores de almacenamiento de vSAN son componentes de software integrados que comunican las funcionalidades del almacén de datos a vCenter Server. Una capacidad de almacenamiento generalmente se representa mediante un par clave-valor, en la que la clave es una propiedad específica que ofrece el almacén de datos. El valor es un número o rango que el almacén de datos puede proporcionar para un objeto aprovisionado, como un objeto del espacio de nombres del directorio principal de la máquina virtual o un disco virtual. También puede usar etiquetas para crear funcionalidades de almacenamiento definidas por el usuario y hacer referencia a ellas al definir una directiva de almacenamiento para una máquina virtual. Para obtener más información sobre cómo aplicar y utilizar etiquetas con los almacenes de datos, consulte la documentación de *Almacenamiento de vSphere*.

Los proveedores de almacenamiento de vSAN informan de un conjunto de funcionalidades de almacenamiento subyacentes a vCenter Server. Asimismo, se comunican con la capa de vSAN para informar de los requisitos de almacenamiento de las máquinas virtuales. Para obtener más información sobre proveedores de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

vSAN registra un proveedor de almacenamiento separado para cada host del clúster de vSAN, mediante la siguiente dirección URL:

http://*host_ip*:8080/version.xml

donde *host_ip* es la dirección IP real del host.

Compruebe que los proveedores de almacenamiento estén registrados.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

Resultados

Los proveedores de almacenamiento para vSAN se muestran en la lista. Cada host posee un proveedor de almacenamiento, pero solo uno está activo. Los proveedores de almacenamiento que pertenecen a los demás hosts están en espera. Si el host que actualmente posee el proveedor de almacenamiento activo presenta un error, se vuelve activo el proveedor de almacenamiento de otro host.

Nota No es posible eliminar del registro de forma manual a los proveedores de almacenamiento que utiliza vSAN. Para quitar los proveedores de almacenamiento de vSAN o eliminarlos del registro, quite los hosts correspondientes del clúster de vSAN y luego vuelva a agregarlos. Asegúrese de que haya al menos un proveedor de almacenamiento activo.

Acerca de la directiva de almacenamiento predeterminada de vSAN

vSAN requiere que a las máquinas virtuales implementadas en los almacenes de datos de vSAN se les asigne, al menos, una directiva de almacenamiento. Al aprovisionar una máquina virtual, si no le asigna una directiva de almacenamiento de manera explícita, se le asigna la directiva de almacenamiento predeterminada de vSAN.

La directiva predeterminada contiene conjuntos de reglas de vSAN y un conjunto de funcionalidades básicas de almacenamiento que generalmente se usan para ubicar las máquinas virtuales implementadas en los almacenes de datos de vSAN.

Tabla 3-2. Especificaciones de la directiva de almacenamiento predeterminada de vSAN

Especificación	Configuración
Nivel primario de errores que se toleran	1
Number of disk stripes per object (Número de fracciones de disco por objeto)	1
Reserva de Flash Read Cache o capacidad flash utilizada para la memoria caché de lectura	0
Reserva de espacio de objetos	Aprovisionamiento fino
Force provisioning (Forzar aprovisionamiento)	No

Si desea revisar las opciones de configuración de la directiva de almacenamiento predeterminada de máquina virtual, desplácese hasta **Directivas de almacenamiento de máquina virtual** > **Directiva de almacenamiento predeterminada de vSAN** > **Administrar** > **Conjunto de reglas 1: vSAN**.

Para obtener mejores resultados, considere la posibilidad de crear y usar sus propias directivas de almacenamiento de máquina virtual, aunque los requisitos de la directiva sean iguales a los definidos en la directiva de almacenamiento predeterminada. Para obtener información sobre cómo crear una directiva de almacenamiento de máquina virtual definida por el usuario, consulte Definir una directiva de almacenamiento de vSAN mediante vSphere Client.

Cuando se asigna una directiva de almacenamiento definida por el usuario a un almacén de datos, vSAN aplica la configuración de la directiva definida por el usuario al almacén de datos especificado. En cualquier momento dado, puede asignar una sola directiva de almacenamiento de máquina virtual como la directiva predeterminada para el almacén de datos de vSAN.

Características

Las características siguientes se aplican a la directiva de almacenamiento predeterminada de vSAN.

- La directiva de almacenamiento predeterminada de vSAN se asignará a todos los objetos de máquina virtual si no se asigna ninguna otra directiva de vSAN al aprovisionar una máquina

virtual. El cuadro de texto **Directiva de almacenamiento de máquina virtual** se configura como **Valor predeterminado de almacén de datos** en la página Seleccionar almacenamiento. Para obtener más información sobre el uso de las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

Nota Los objetos de intercambio de máquina virtual y de memoria de máquina virtual reciben la directiva de almacenamiento de vSAN predeterminada cuando **Forzar aprovisionamiento** se establece en **Sí**.

- La directiva predeterminada de vSAN solo se aplica a los almacenes de datos de vSAN. No es posible aplicar la directiva de almacenamiento predeterminada a almacenes de datos no pertenecientes a vSAN (por ejemplo, un almacén de datos de NFS o VMFS).
- Debido a que la directiva de almacenamiento predeterminada de la máquina virtual es compatible con cualquier almacén de datos de vSAN en vCenter Server, puede transferir los objetos de máquinas virtuales aprovisionados con la directiva predeterminada a cualquier almacén de datos de vSAN en vCenter Server.
- Puede clonar la directiva predeterminada y usarla como plantilla para crear una directiva de almacenamiento definida por el usuario.
- Si tiene el privilegio Perfil de almacenamiento.Vista, puede editar la directiva predeterminada. Debe tener al menos un clúster habilitado para vSAN que contenga un host como mínimo. Por lo general, la configuración de la directiva de almacenamiento predeterminada no se modifica.
- No es posible editar el nombre ni la descripción de la directiva predeterminada, ni tampoco la especificación del proveedor de almacenamiento de vSAN. Todos los demás parámetros, incluidas las reglas de la directiva, pueden editarse.
- No es posible eliminar la directiva predeterminada.
- La directiva de almacenamiento predeterminada se asigna cuando la directiva que asigna durante el aprovisionamiento de máquinas virtuales no incluye reglas específicas para vSAN.

Cambiar la directiva de almacenamiento predeterminada de los almacenes de datos de vSAN

Es posible cambiar la directiva de almacenamiento predeterminada para un almacén de datos de vSAN seleccionado.

Requisitos previos

Compruebe que la directiva de almacenamiento de máquina virtual que desea asignar como la directiva predeterminada para el almacén de datos de vSAN cumpla con los requisitos de las máquinas virtuales del clúster de vSAN.

Procedimiento

1 Vaya hasta el almacén de datos de vSAN.

2 Haga clic en **Configurar**.

3 En **General**, haga clic en el botón **Editar** de la directiva de almacenamiento predeterminada y seleccione la directiva de almacenamiento que desea asignar como la predeterminada para el almacén de datos de vSAN.

   Puede elegir entre una lista de directivas de almacenamiento compatibles con el almacén de datos de vSAN, como la directiva de almacenamiento predeterminada de vSAN y las directivas de almacenamiento definidas por el usuario que contienen conjuntos de reglas de vSAN definidos.

4 Seleccione una directiva y haga clic en **OK** (Aceptar).

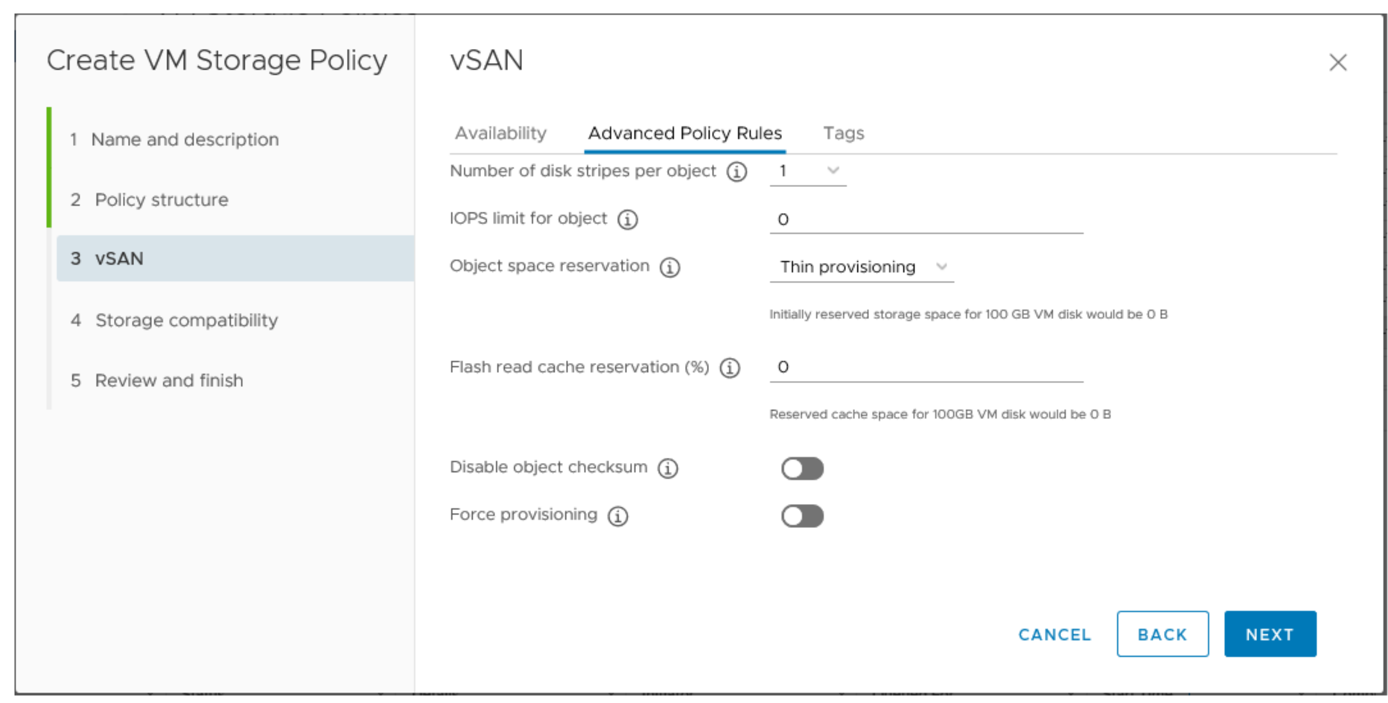
   La directiva de almacenamiento se aplica como la directiva predeterminada al aprovisionar las nuevas máquinas virtuales sin especificar una directiva de almacenamiento de manera explícita para un almacén de datos.

Pasos siguientes

Puede definir una nueva directiva de almacenamiento para máquinas virtuales. Consulte Definir una directiva de almacenamiento de vSAN mediante vSphere Client.

Definir una directiva de almacenamiento de vSAN mediante vSphere Client

Es posible crear una directiva de almacenamiento en la que se definan los requisitos de almacenamiento para una máquina virtual y sus discos virtuales. En esta directiva, se debe hacer referencia a las capacidades de almacenamiento que admite el almacén de datos de vSAN.



Requisitos previos

- Compruebe que el proveedor de almacenamiento de vSAN esté disponible. Consulte Ver los proveedores de almacenamiento de vSAN.
- Privilegios requeridos: **Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles** y **Almacenamiento basado en perfiles.Actualización de almacenamiento basado en perfiles**

Procedimiento

1. Desplácese hasta **Directivas y perfiles** y haga clic en **Directivas de almacenamiento de máquina virtual**.
2. Haga clic en el icono **Create a new VM storage policy** (Crear una nueva directiva de almacenamiento de máquina virtual) ().
3. En la página de nombre y descripción, seleccione un vCenter Server.
4. Escriba un nombre y una descripción para la directiva de almacenamiento y haga clic en **Siguiente**.
5. En la página Estructura de directiva, seleccione Habilitar reglas para el almacenamiento "vSAN" y haga clic en **Siguiente**.

6 En la página vSAN, defina el conjunto de reglas de la directiva y haga clic en **Siguiente**.

   a En la pestaña Disponibilidad, defina las opciones **Tolerancia ante desastres de sitio** y **Errores que se toleran**.

      Las opciones de disponibilidad definen las reglas de los niveles principal y secundario de errores que se toleran, la localidad de datos y el método de tolerancia a errores.

      - En **Tolerancia ante desastres de sitio**, se define el tipo de tolerancia ante errores en el sitio que se utilizará para objetos de máquina virtual.
      - En **Errores que se toleran**, se definen el número de errores de host y de dispositivo que un objeto de máquina virtual puede tolerar y el método de replicación de datos.

      Por ejemplo, si elige **Creación de reflejo de sitio doble** y **2 errores - RAID-6 (codificación de borrado)**, vSAN configura las reglas de directivas siguientes:

      - Nivel primario de errores que se toleran: 1
      - Nivel secundario de errores que se toleran: 2
      - Localidad de datos: Ninguna
      - Método de tolerancia a errores: RAID-5/6 (codificación de borrado) - Capacidad

   b En la pestaña Reglas de directivas avanzadas, defina las reglas de directivas avanzadas (por ejemplo, el número de fracciones de disco por objeto y los límites de IOPS).

   c En la pestaña Etiquetas, haga clic en **Agregar regla de etiqueta** y defina las opciones de la regla de etiqueta.

      Asegúrese de proporcionar valores que se ubiquen dentro del rango de valores anunciado por las funcionalidades de almacenamiento del almacén de datos de vSAN.

7 En la página de compatibilidad de almacenamiento, revise la lista de almacenes de datos que coinciden con esta directiva y haga clic en **Siguiente**.

   Para cumplir las condiciones, un almacén de datos no necesita satisfacer todos los conjuntos de reglas incluidos en la directiva. El almacén de datos debe satisfacer al menos uno de los conjuntos de reglas y todas las reglas de dicho conjunto. Verifique que el almacén de datos de vSAN cumpla con los requisitos establecidos en la directiva de almacenamiento y que figure en la lista de almacenes de datos compatibles.

8 En la página Revisar y finalizar, revise la configuración de la directiva y haga clic en **Finalizar**.

Resultados

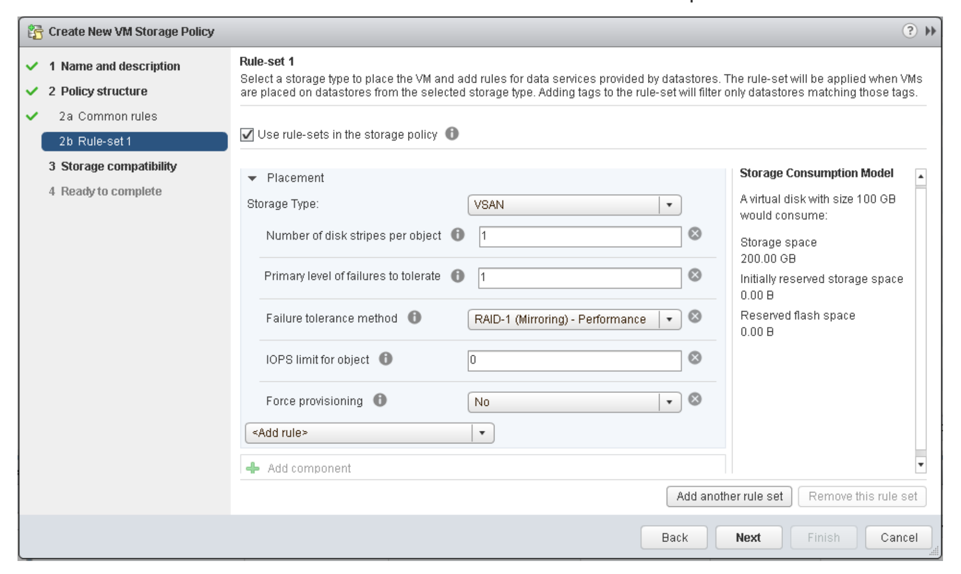
La nueva directiva se agrega a la lista.

Pasos siguientes

Asigne esta directiva a una máquina virtual y sus discos virtuales. vSAN coloca los objetos de máquina virtual según los requisitos especificados en la directiva. Para obtener información sobre cómo aplicar directivas de almacenamiento a objetos de máquinas virtuales, consulte el documento *Almacenamiento de vSphere*.

Definir una directiva de almacenamiento de vSAN con vSphere Web Client

Es posible crear una directiva de almacenamiento en la que se definan los requisitos de almacenamiento para una máquina virtual y sus discos virtuales. En esta directiva, se debe hacer referencia a las funcionalidades de almacenamiento que admite el almacén de datos de vSAN.



Requisitos previos

- Compruebe que el proveedor de almacenamiento de vSAN esté disponible. Consulte Ver los proveedores de almacenamiento de vSAN.
- Asegúrese de que estén habilitadas las directivas de almacenamiento para las máquinas virtuales. Para obtener información sobre las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere*.
- Privilegios requeridos: **Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles** y **Almacenamiento basado en perfiles.Actualización de almacenamiento basado en perfiles**

Procedimiento

1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles** y, a continuación, en **Directivas de almacenamiento de máquina virtual**.

2 Haga clic en el icono **Create a new VM storage policy** (Crear una nueva directiva de almacenamiento de máquina virtual) ( ).

3 En la página de nombre y descripción, seleccione un vCenter Server.

4 Escriba un nombre y una descripción para la directiva de almacenamiento y haga clic en **Next** (Siguiente).

5 En la página de estructura de la directiva, haga clic en **Siguiente**.

6 En la página **Reglas comunes para los servicios de datos proporcionados por los hosts**, haga clic en **Siguiente**.

7 En la página Conjunto de reglas 1, defina el primer conjunto de reglas.

   a Marque la casilla **Usar conjuntos de reglas en la directiva de almacenamiento**.

   b Seleccione **VSAN** en el menú desplegable **Tipo de almacenamiento**.

      La página se ampliará a medida que se agreguen reglas para el almacén de datos de vSAN.

   c Seleccione una regla del menú desplegable **Agregar regla**.

      Asegúrese de proporcionar valores que se ubiquen dentro del rango de valores anunciado por las funcionalidades de almacenamiento del almacén de datos de vSAN.

      Desde el modelo de consumo de almacenamiento, puede consultar el tamaño de disco virtual disponible y los requisitos correspondientes de capacidad y memoria caché, incluido el espacio de almacenamiento reservado que potencialmente podrían consumir las máquinas virtuales al aplicar la directiva de almacenamiento.

   d (opcional) Agregue funcionalidades basadas en etiquetas.

8 (opcional) Haga clic en el botón **Agregar otro conjunto de reglas** para agregar otro conjunto de reglas.

9 Haga clic en **Siguiente**.

10 En la página de compatibilidad de almacenamiento, revise la lista de almacenes de datos que coinciden con esta directiva y haga clic en **Siguiente**.

   Para cumplir las condiciones, un almacén de datos no necesita satisfacer todos los conjuntos de reglas incluidos en la directiva. El almacén de datos debe satisfacer al menos uno de los conjuntos de reglas y todas las reglas de dicho conjunto. Verifique que el almacén de datos de vSAN cumpla con los requisitos establecidos en la directiva de almacenamiento y que figure en la lista de almacenes de datos compatibles.

11 En la página de finalización, revise la configuración de la directiva y haga clic en **Finalizar**.

Resultados

La nueva directiva se agrega a la lista.

Pasos siguientes

Asigne esta directiva a una máquina virtual y sus discos virtuales. vSAN coloca los objetos de máquina virtual según los requisitos especificados en la directiva. Para obtener información sobre cómo aplicar directivas de almacenamiento a objetos de máquinas virtuales, consulte el documento *Almacenamiento de vSphere*.

Expandir y administrar un clúster de vSAN

4

Después de configurar el clúster de vSAN, puede agregar hosts y dispositivos de capacidad, quitar hosts y dispositivos, y administrar escenarios de errores.

Este capítulo incluye los siguientes temas:

Expandir un clúster de vSAN

Puede expandir un clúster existente de vSAN agregando hosts o dispositivos a los hosts existentes sin interrumpir las operaciones en curso.

Use uno de los siguientes métodos para expandir el clúster de vSAN.

- Agregue al clúster hosts ESXi nuevos que estén configurados mediante dispositivos compatibles de memoria caché y de capacidad. Consulte Agregar un host al clúster de vSAN. Al agregar un dispositivo o un host con capacidad, vSAN no distribuye los datos automáticamente al nuevo dispositivo agregado. Para permitir que vSAN distribuya los datos a los dispositivos agregados recientemente, debe volver a equilibrar manualmente el clúster mediante la herramienta Ruby vSphere Console (RVC). Consulte "Redistribución manual" en *Supervisar vSAN y solucionar sus problemas*.
- Transfiera hosts existentes de ESXi al clúster de vSAN mediante el perfil de host. Consulte Configurar hosts mediante un perfil de host. Los nuevos miembros del clúster agregan capacidad informática y de almacenamiento. Debe crear manualmente un subconjunto de grupos de discos a partir de los dispositivos de capacidad locales en el host recién agregado. Consulte Crear un grupo de discos en un host de vSAN.

Verifique que los componentes de hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento que planea usar estén certificados y se enumeren en la Guía de compatibilidad de VMware, en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php. Al agregar dispositivos de capacidad, asegúrese de que los dispositivos no tengan formato ni particiones a fin de que vSAN pueda reconocer y reclamar los dispositivos.

- Agregue nuevos dispositivos de capacidad a hosts ESXi que sean miembros del clúster. Debe agregar el dispositivo manualmente al grupo de discos en el host. Consulte Agregar dispositivos al grupo de discos.

Expandir la capacidad y el rendimiento de un clúster de vSAN

Si el clúster de vSAN se está quedando sin capacidad de almacenamiento o si detecta una merma en el rendimiento del clúster, puede expandir la capacidad y el rendimiento del clúster.

- Expanda la capacidad de almacenamiento del clúster agregando dispositivos de almacenamiento a los grupos de discos existentes o agregando grupos de discos. Los grupos de discos nuevos requieren dispositivos flash para la memoria caché. Para obtener información sobre cómo agregar dispositivos a grupos de discos, consulte Agregar dispositivos al grupo de discos. Agregar dispositivos de capacidad sin aumentar la memoria caché puede reducir la proporción entre caché y capacidad a un nivel no compatible. Consulte "Consideraciones de diseño para dispositivos flash de almacenamiento en caché en vSAN" en *Administrar VMware vSAN*.
- Para mejorar el rendimiento del clúster, agregue al menos un dispositivo de memoria caché (flash) y un dispositivo de capacidad (flash o disco magnético) a una controladora de E/S de almacenamiento existente o a un host nuevo. También puede agregar uno o varios hosts con grupos de discos para producir el mismo impacto en el rendimiento después de que vSAN complete una redistribución proactiva en el clúster de vSAN.

Si bien los hosts solo con recursos informáticos pueden existir en un clúster de vSAN y pueden consumir capacidad de otros hosts del clúster, agregue hosts con una configuración uniforme para lograr un funcionamiento eficiente. Para obtener los mejores resultados, agregue hosts con dispositivos de memoria caché y de capacidad para expandir la capacidad del clúster. A pesar de que es mejor utilizar dispositivos idénticos o similares en los grupos de discos, cualquier dispositivo incluido en la HCL de vSAN es compatible. Intente distribuir la capacidad de manera uniforme entre los hosts y los grupos de discos. Para obtener información sobre cómo agregar dispositivos a grupos de discos, consulte Agregar dispositivos al grupo de discos.

Después de expandir la capacidad del clúster, realice una redistribución manual para distribuir equitativamente los recursos en el clúster. Para obtener más información, consulte "Redistribución manual" en *Supervisar vSAN y solucionar sus problemas*.

Utilizar el inicio rápido para agregar hosts a un clúster de vSAN

Si configuró el clúster de vSAN a través del inicio rápido, puede usar el flujo de trabajo de inicio rápido para agregar hosts y dispositivos de almacenamiento al clúster.

Cuando agregue nuevos hosts al clúster de vSAN, puede utilizar el asistente de configuración de clúster para completar la configuración del host. Para obtener más información acerca del inicio rápido, consulte "Usar el inicio rápido para configurar y expandir un clúster de vSAN" en *Planificar e implementar vSAN*.

Nota Si ejecuta vCenter Server en un host del clúster, no es necesario colocar el host en modo de mantenimiento cuando lo agrega a un clúster con el flujo de trabajo de inicio rápido. El host que contiene la máquina virtual de vCenter Server debe ejecutar ESXi 6.5 EP2 o una versión posterior. El mismo host también puede estar ejecutando una instancia de Platform Services Controller. Todas las demás máquinas virtuales en el host deben estar apagadas.

Requisitos previos

El flujo de trabajo de inicio rápido debe estar disponible para el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster en vSphere Client.

2 Haga clic en la pestaña Configurar y seleccione **Configuración > Inicio rápido**.

3 En la tarjeta Agregar hosts, haga clic en **Agregar** para abrir el asistente Agregar hosts.

   a En la página Agregar hosts, introduzca la información de nuevos hosts, o bien haga clic en Hosts existentes y seleccione los hosts que aparecen en el inventario.

   b En la página Resumen del host, compruebe la configuración del host.

   c En la página Listo para finalizar, haga clic en **Finalizar**.

4 En la tarjeta Configuración del clúster, haga clic en **Configurar** para abrir el asistente de configuración del clúster.

   a (Opcional) En la página Tráfico de vMotion, introduzca la información de dirección IP del tráfico de vMotion.

   b En la página Tráfico de almacenamiento, introduzca la información de dirección IP del tráfico de almacenamiento.

   c (opcional) En la página Reclamar discos, seleccione los discos en cada host nuevo.

   d (opcional) En la página Crear dominios de errores, mueva los nuevos hosts a sus correspondientes dominios de errores.

   Para obtener más información sobre los dominios de errores, consulte Administrar dominios de errores en clústeres de vSAN.

   e En la página Listo para completar, compruebe la configuración del clúster y haga clic en **Finalizar**.

Agregar un host al clúster de vSAN

Puede agregar hosts ESXi a un clúster de vSAN en ejecución sin interrumpir las operaciones en curso. Los recursos del host nuevo se asociarán al clúster.

Requisitos previos

- Compruebe que los recursos, incluidos los controladores, el firmware y las controladoras de E/S de almacenamiento, aparezcan en el sitio web de la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php.
- VMware recomienda crear hosts configurados de manera uniforme en el clúster de vSAN a fin de que pueda obtener una distribución homogénea de los componentes y los objetos en los dispositivos del clúster. Sin embargo, pueden haber situaciones en las que el clúster no esté equilibrado de manera homogénea, especialmente durante el mantenimiento o si se sobreasigna la capacidad del almacén de datos de vSAN con implementaciones excesivas de máquinas virtuales.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic con el botón derecho en el clúster y seleccione **Agregar hosts**. Se mostrará el asistente Agregar hosts.

Opción	Descripción
Nuevos hosts	a Introduzca el nombre de host o la dirección IP. b Introduzca el nombre de usuario y la contraseña asociados con el host.
Hosts existentes	a Seleccione los hosts que agregó previamente a vCenter Server.

3 Haga clic en **Next** (Siguiente).

4 Consulte la información de resumen y haga clic en **Next** (Siguiente).

5 Revise la configuración y haga clic en **Finish** (Finalizar).

El host se agrega al clúster.

Pasos siguientes

Verifique que la comprobación de estado del equilibrio de disco de vSAN sea de color verde. Si la comprobación de estado del equilibrio de disco emite una advertencia, ejecute una operación de redistribución manual fuera de las horas punta. Para obtener más información, consulte "Redistribución manual" en *Supervisar vSAN y solucionar sus problemas*.

Para obtener más información sobre la configuración de clústeres de vSAN y la solución de problemas, consulte "Problemas de configuración del clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*.

Configurar hosts mediante un perfil de host

Cuando se tienen varios hosts en el clúster de vSAN, es posible utilizar el perfil de un host de vSAN existente para configurar el resto de los hosts del clúster de vSAN.

El perfil de host incluye información sobre la configuración de almacenamiento, la configuración de red y otras características del host. Si piensa crear un clúster con muchos hosts, por ejemplo, 8, 16, 32 o 64 hosts, utilice la característica de perfil de host. Los perfiles de host le permiten agregar más de un host a la vez al clúster de vSAN.

Requisitos previos

- Compruebe que el host esté en modo de mantenimiento.
- Compruebe que los componentes de hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento se enumeren en la Guía de compatibilidad de VMware en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.

Procedimiento

1 Cree un perfil de host.

   a Desplácese hasta la vista de perfiles de host.

   b Haga clic en el icono **Extract Profile from a Host** (Extraer perfil de un host) ( ).

   c Seleccione el host que desea utilizar como host de referencia y haga clic en **Siguiente**.

   El host seleccionado debe ser un host activo.

   d Escriba un nombre y una descripción para nuevo perfil y haga clic en **Siguiente**.

   e Revise la información de resumen del nuevo perfil de host y haga clic en **Finalizar**.

   El nuevo perfil aparece en la lista Host Profile (Perfil del host).

2 Asocie el host al perfil de host deseado.

   a Desde la lista Perfil en la vista de Host Profiles, seleccione el perfil de host que se debe aplicar al host de vSAN.

   b Haga clic en el icono **Attach/Detach Hosts and clusters to a host profile** (Asociar o separar hosts y clústeres para un perfil de host)().

   c Seleccione el host desde la lista expandida, haga clic en **Asociar** y, a continuación, haga clic en el host que desea asociar con el perfil.

   El host se agrega a la lista Entidades asociadas.

   d Haga clic en **Siguiente**.

   e Haga clic en **Finalizar** para completar la operación de asociación del host con el perfil.

3 Separe del perfil de host el host de vSAN al que se hace referencia.

Cuando se asocia un perfil de host a un clúster, los hosts de ese clúster también se asocian al perfil de host. Sin embargo, cuando el perfil de host se separa del clúster, la asociación entre el host o los hosts incluidos en el clúster y el perfil de host permanece intacta.

a Desde la lista Perfil en la vista Perfiles de host, seleccione el perfil de host que desea separar de un host o un clúster.

b Haga clic en el icono **Attach/Detach Hosts and clusters to a host profile** (Asociar o separar hosts y clústeres para un perfil de host)().

c Seleccione el host o el clúster desde la lista expandida y haga clic en **Separar**.

d Haga clic en **Separar todos** para separar todos los hosts y los clústeres del perfil.

e Haga clic en **Siguiente**.

f Haga clic en **Finish** (Finalizar) para completar la operación de desasociación del host del perfil del host.

4 Compruebe que el host de vSAN cumpla con los requisitos del perfil de host asociado y determine si hay parámetros de configuración diferentes a los especificados en el perfil de host.

a Desplácese hasta un perfil de host.

En la pestaña **Objetos**, se enumeran todos los perfiles de host, la cantidad de hosts asociados con el perfil de host y los resultados resumidos de la última comprobación de cumplimiento.

b Haga clic en el icono **Check Host Profile Compliance** (Comprobar cumplimiento de perfil de host) ().

Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento). Expanda la jerarquía de objetos y seleccione el host no compatible. Los parámetros con diferencias se muestran en la ventana Cumplimiento, debajo de la jerarquía.

Si se produce un error de cumplimiento, use la acción Corregir para aplicar la configuración del perfil de host al host. Esta acción cambia todos los parámetros administrados por el perfil de host por los valores contenidos en el perfil de host asociado al host.

c Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento).

d Expanda la jerarquía de objetos y seleccione el host con error.

Los parámetros con diferencias se muestran en la ventana Cumplimiento, debajo de la jerarquía.

5 Corrija el host para solucionar los errores de cumplimiento.

   a Seleccione la pestaña **Supervisar** y haga clic en **Cumplimiento**.

   b Haga clic con el botón derecho en los hosts y seleccione **All vCenter Actions (Todas las acciones de vCenter) > Host Profiles (Perfiles de host) > Remediate (Corregir)**.

      Puede personalizar el host para actualizar o cambiar los parámetros de entrada del usuario de las directivas de perfiles de host.

   c Haga clic en **Siguiente**.

   d Revise las tareas necesarias para corregir el perfil de host y haga clic en **Finalizar**.

   El host forma parte del clúster de vSAN y sus recursos están accesibles para el clúster de vSAN. El host también puede acceder a todas las directivas de E/S de almacenamiento de vSAN existentes en el clúster de vSAN.

Trabajar con el modo de mantenimiento

Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento.

Al trabajar con el modo de mantenimiento, tenga en cuenta las siguientes directrices:

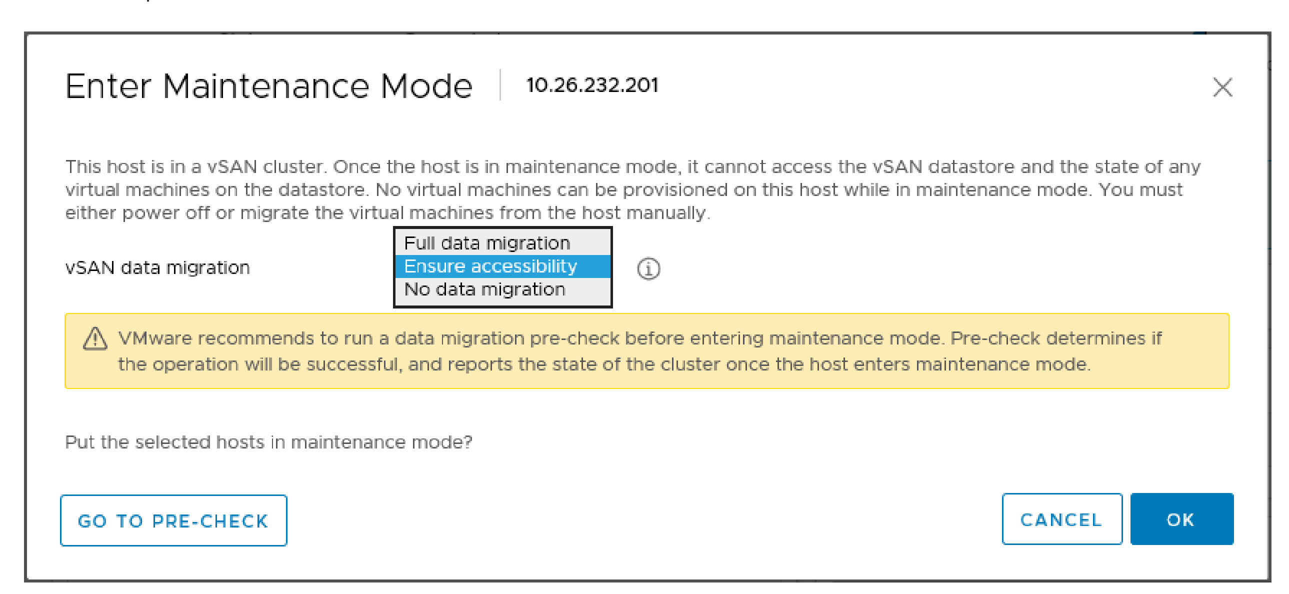
- Cuando coloque un host ESXi en el modo de mantenimiento, deberá seleccionar un modo de evacuación de datos, como **Ensure accessibility** (Garantizar disponibilidad) o **Full data migration** (Migración de datos completa).
- Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar almacenamiento al clúster.
- Es posible que los recursos informáticos de una máquina virtual no estén en el host que se va a colocar en el modo de mantenimiento, y los recursos de almacenamiento de las máquinas virtuales pueden estar ubicados en cualquier parte del clúster.
- El modo **Ensure accessibility** (Garantizar disponibilidad) es más rápido que el modo **Full data migration** (Migración de datos completa), ya que **Ensure accessibility** (Garantizar disponibilidad) solo migra los componentes de los hosts que son imprescindibles para la ejecución de las máquinas virtuales. En este modo, si se experimenta un error, se ve afectada la disponibilidad de la máquina virtual. Cuando se selecciona el modo **Ensure accessibility** (Garantizar disponibilidad), los datos no se reprotegen durante un error y puede experimentarse una pérdida de datos inesperada.
- Cuando se selecciona el modo **Migración de datos completa**, los datos se reprotegen automáticamente contra errores, si hay recursos disponibles y el **Nivel primario de errores que se toleran** está establecido en 1 o más. En este modo, se migran todos los componentes del host y, según la cantidad de datos que haya en el host, es posible que la migración tarde más. En el modo **Full data migration** (Migración de datos completa), las máquinas virtuales pueden tolerar errores, incluso durante el mantenimiento planificado.

- Al trabajar con un clúster de tres hosts, no puede colocar un servidor en el modo de mantenimiento con **Full data migration** (Migración de datos completa). Para obtener la disponibilidad máxima, debe considerar la posibilidad de diseñar un clúster con cuatro hosts o más.

Antes de colocar un host en el modo de mantenimiento, debe comprobar lo siguiente:

- Si utiliza el modo **Migración de datos completa**, compruebe que el clúster disponga de suficientes hosts y capacidad disponible para cumplir con los requisitos de la directiva **Nivel primario de errores que se toleran**.
- Compruebe que exista suficiente capacidad flash en los hosts restantes para controlar las reservas de Flash Read Cache. Ejecute el comando de RVC `vsan.whatif_host_failures` para analizar el uso de capacidad actual por host y determinar si un único error de host podría causar que se agote el espacio del clúster y afectar la capacidad del clúster, la reserva de memoria caché y los componentes del clúster. Para obtener información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Verifique que disponga de suficientes dispositivos de capacidad en los hosts restantes para controlar los requisitos de la directiva de ancho de las fracciones, si está seleccionada.
- Asegúrese de disponer de suficiente capacidad libre en los hosts restantes para controlar la cantidad de datos que deben migrarse desde el host que va a entrar en modo de mantenimiento.

Ejecute la comprobación previa de migración de datos para verificar el efecto causado en el clúster al poner el host en modo de mantenimiento.



En el cuadro de diálogo Confirmar modo de mantenimiento se proporciona información para guiarle durante las actividades de mantenimiento. Puede ver el impacto de cada opción de evacuación de datos.

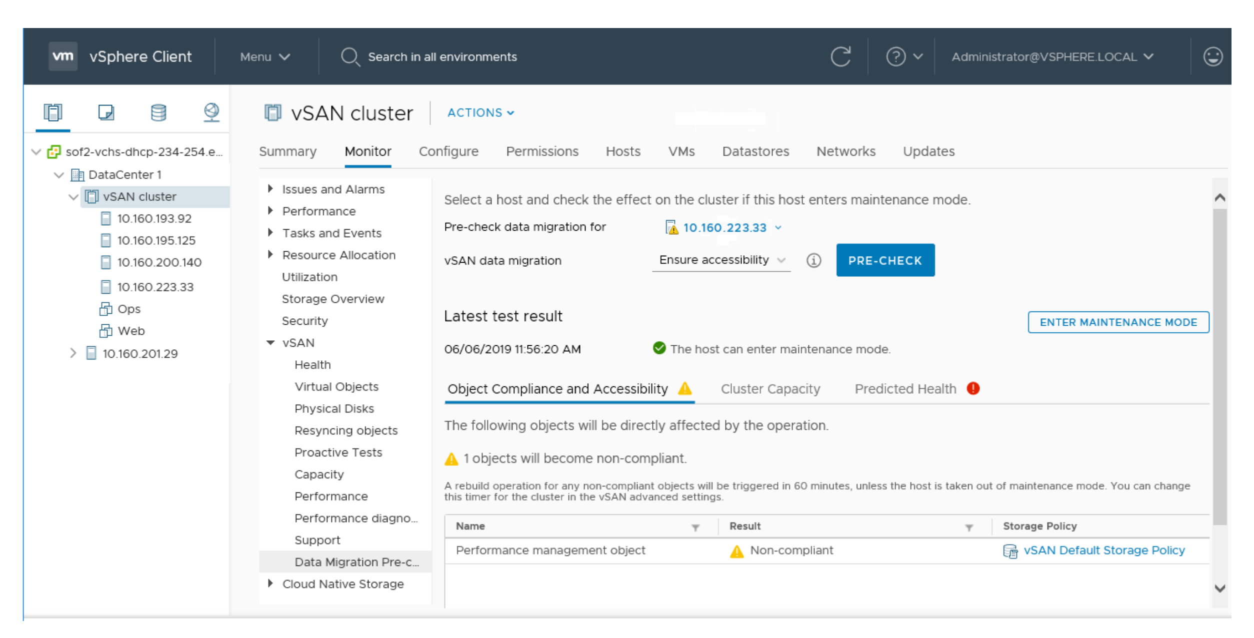
- Si hay o no suficiente capacidad para realizar la operación.
- Cuántos datos se moverán.

- Cuántos objetos dejarán de cumplir con las normas.
- Cuántos objetos se volverán inaccesibles.

Comprobar las capacidades de migración de datos de un miembro

Utilice la comprobación previa de migración de datos para determinar el impacto de las opciones de migración de datos al poner un host en modo de mantenimiento o quitarlo del clúster.

Antes de poner un host de vSAN en modo de mantenimiento, ejecute la comprobación previa de migración de datos. Los resultados de la prueba proporcionarán información para determinar el impacto sobre la capacidad del clúster, las comprobaciones de estado previsto y los objetos que se apartarán del cumplimiento. Si se espera que la operación no se realice correctamente, la comprobación previa proporcionará información sobre los recursos necesarios.



Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña Supervisar.
3. En vSAN, haga clic en **Comprobación previa a la migración de datos**.
4. Seleccione un host, una opción de migración de datos y haga clic en **Comprobación previa**.

   vSAN ejecutará las pruebas de comprobación previa de migración de datos.
5. Vea los resultados de la prueba.

   Los resultados de la comprobación previa muestran si el host puede entrar en modo de mantenimiento de forma segura.

   - La pestaña Conformidad y accesibilidad de objetos muestra los objetos que pueden presentar problemas después de la migración de datos.

- La pestaña Capacidad del clúster muestra el impacto de la migración de datos en el clúster de vSAN antes y después de realizar la operación.
- La pestaña Estado previsto muestra las comprobaciones de estado que podrían verse afectadas por la migración de datos.

Pasos siguientes

Si la comprobación previa indica que puede poner el host en modo de mantenimiento, puede hacer clic en **Entrar en modo de mantenimiento** para migrar los datos y poner el host en modo de mantenimiento.

Poner un miembro de un clúster de vSAN en modo de mantenimiento

Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento. Cuando coloque un host en el modo de mantenimiento, deberá seleccionar un modo de evacuación de datos, como **Garantizar disponibilidad** o **Migración de datos completa**.

Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar capacidad al clúster.

Todos los destinos de iSCSI de vSAN atendidos por este host se transfieren a otros hosts del clúster y, por tanto, el iniciador iSCSI se redirecciona al nuevo propietario de destino.

Requisitos previos

Compruebe que el entorno cuente con las funcionalidades necesarias para la opción seleccionada.

Procedimiento

1 Haga clic con el botón derecho en el host y seleccione **Maintenance Mode > Enter Maintenance Mode** (Modo de mantenimiento > Entrar en modo de mantenimiento).

2 Seleccione un modo de evacuación de datos y haga clic en **Aceptar**.

Opción	Descripción
Garantizar disponibilidad	Esta es la opción predeterminada. Al apagar el host o quitarlo del clúster, vSAN se asegura de que todas las máquinas virtuales que están accesibles en este host permanezcan accesibles. Seleccione esta opción si desea quitar el host temporalmente del clúster, por ejemplo, para instalar actualizaciones, y tiene planificado restituir el host en el clúster. Esta opción no es adecuada si se pretende quitar el host del clúster de manera permanente. Por lo general, solamente se requiere una evacuación parcial de datos. Sin embargo, es posible que la máquina virtual ya no cumpla por completo con la directiva de almacenamiento de la máquina virtual durante la evacuación. Eso significa que es posible que no tenga acceso a todas las réplicas. Si se produce un error mientras el host está en modo de mantenimiento y **Nivel primario de errores que se toleran** se establece como 1, es posible que se experimente una pérdida de datos en el clúster. **Nota** Este es el único modo de evacuación disponible si se trabaja con un clúster de tres hosts o con un clúster de vSAN configurado con tres dominios de errores.
Migración de datos completa	vSAN evacua todos los datos a otros hosts del clúster y mantiene el estado actual de cumplimiento de objetos. Seleccione esta opción si tiene planificado migrar el host de manera permanente. Al evacuar datos del último host del clúster, asegúrese de migrar las máquinas virtuales a otro almacén de datos y luego ponga el host en modo de mantenimiento. Este modo de evacuación genera el mayor volumen de transferencia de datos y consume más tiempo y recursos. Todos los componentes en el almacenamiento local del host seleccionado se migran a otra ubicación del clúster. Cuando el host entra en modo de mantenimiento, todas las máquinas virtuales pueden acceder a los componentes de almacenamiento y siguen cumpliendo con las directivas de almacenamiento que tienen asignadas. **Nota** Si hay objetos en estado de disponibilidad reducida, este modo mantiene este estado de cumplimiento y no garantiza que los objetos pasen a cumplir los requisitos. Si no es posible acceder a un objeto de máquina virtual que tiene datos en el host y no se evacua por completo, el host no podrá entrar en el modo de mantenimiento.
Sin migración de datos	vSAN no evacúa datos de este host. Al apagar el host o quitarlo del clúster, es posible que algunas máquinas virtuales dejen de estar accesibles.

Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con hosts, entre ellas, la imposibilidad de usar el modo **Migración de datos completa** o de reproteger los datos después de un error.

Como alternativa, puede poner un host en modo de mantenimiento mediante ESXCLI. Antes de poner un host en este modo, asegúrese de apagar las máquinas virtuales que se ejecutan en el host.

Para entrar en modo de mantenimiento, ejecute el siguiente comando en el host:

```
esxcli system maintenanceMode set --enable 1
```

Para verificar el estado del host, ejecute el siguiente comando:

```
esxcli system maintenanceMode get
```

Para salir del modo de mantenimiento, ejecute el siguiente comando:

```
esxcli system maintenanceMode set --enable 0
```

Pasos siguientes

Puede hacer un seguimiento del progreso de la migración de datos en el clúster. Consulte "Supervisar las tareas de resincronización en el clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*.

Administrar dominios de errores en clústeres de vSAN

Los dominios de errores son una protección contra los errores en el bastidor o el chasis si el clúster de vSAN abarca varios bastidores o chasis de servidores blade. Puede crear dominios de errores, y agregar uno o varios hosts a cada dominio de errores.

Un dominio de errores consta de uno o varios hosts de vSAN agrupados según su ubicación física en el centro de datos. Cuando se configuran, los dominios de errores permiten que vSAN tolere errores de bastidores físicos completos, así como errores de un único host, un dispositivo de capacidad, un vínculo de red o un conmutador de red dedicado a un dominio de errores.

La directiva **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) depende de la cantidad de errores que una máquina virtual se aprovisionó para tolerar. Cuando se configura una máquina virtual con **Nivel primario de errores que se toleran** establecido como 1 `(PFTT=1)`, vSAN puede tolerar un solo error de cualquier tipo y de cualquier componente en un dominio de errores, incluidos errores en un bastidor completo.

Cuando se configuran dominios de errores en un bastidor y se aprovisiona una máquina virtual nueva, vSAN garantiza que los objetos de protección como las réplicas y los testigos se ubiquen en dominios de errores diferentes. Por ejemplo, si la directiva de almacenamiento de una máquina virtual tiene el atributo **Nivel primario de errores que se toleran** establecido en N `(PFTT=n)`, vSAN requiere un mínimo de `2*n+1` dominios de errores en el clúster. Cuando se aprovisionan máquinas virtuales en un clúster con dominios de errores que usan esta directiva, las copias de los objetos asociados de máquinas virtuales se almacenan en bastidores separados.

Se requieren al menos tres dominios de errores para admitir que PFTT sea igual a 1. Para obtener mejores resultados, configure cuatro dominios de errores o más en el clúster. Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con hosts, entre ellas, la imposibilidad de reproteger datos después de un error y de usar el modo **Full data migration** (Migración de datos completa). Para obtener información sobre cómo diseñar dominios de errores y definir su tamaño, consulte "Diseñar dominios de errores de vSAN y definir su tamaño" en *Planificar e implementar vSAN*.

Piense en un escenario en el cual tiene un clúster de vSAN con 16 hosts. Los hosts se distribuyen entre cuatro bastidores (es decir, cuatro hosts por bastidor). Para tolerar errores en un bastidor completo, cree un dominio de errores para cada bastidor. Puede configurar un clúster con esa capacidad con **Nivel primario de errores que se toleran** establecido como 1. Si desea establecer **Nivel primario de errores que se toleran** como 2, configure cinco dominios de errores en el clúster.

Cuando se produce un error en un bastidor, todos los recursos, incluida la CPU y la memoria en el bastidor, dejan de estar disponibles en el clúster. Para reducir el impacto de un posible error de bastidor, configure dominios de errores de menor tamaño. Al aumentar el número de dominios de errores, la cantidad total de recursos disponibles aumenta en el clúster después de un error de bastidor.

Al trabajar con dominios de errores, siga las prácticas recomendadas.

- Configure un mínimo de tres dominios de errores en el clúster de vSAN. Para obtener mejores resultados, configure cuatro dominios de errores.
- Un host que no forma parte de ningún dominio de errores se considera que reside en su propio dominio de errores de host individual.
- No es necesario asignar cada host de vSAN a un dominio de errores. Si decide usar dominios de errores para proteger el entorno de vSAN, considere la posibilidad de crear dominios de errores del mismo tamaño.
- Cuando se transfieren a otro clúster, los hosts de vSAN retienen las asignaciones de dominios de errores.
- Al diseñar un dominio de errores, coloque una cantidad de hosts uniforme en cada dominio de errores.

  Para obtener instrucciones sobre el diseño de dominios de errores, consulte "Diseñar dominios de errores de vSAN y definir su tamaño" en *Planificar e implementar vSAN*.
- Puede agregar cualquier cantidad de hosts a un dominio de errores. Cada dominio de errores debe contener al menos un host.

Crear un nuevo dominio de errores en un clúster de vSAN

Para garantizar que los objetos de máquinas virtuales sigan ejecutándose correctamente durante un error de un bastidor, puede agrupar los hosts en distintos dominios de errores.

Al aprovisionar una máquina virtual en el clúster con dominios de errores, vSAN distribuye los componentes de protección, como los testigos y las réplicas de los objetos de máquinas virtuales entre distintos dominios de errores. Como consecuencia, el entorno de vSAN puede tolerar errores de bastidores completos, además de errores individuales en un host, en un disco de almacenamiento o en una red.

Requisitos previos

- Elija un nombre único para el dominio de errores. vSAN no admite nombres duplicados de dominios de errores en un clúster.
- Compruebe la versión de los hosts ESXi. Solamente puede incluir hosts de la versión 6.0 o posteriores en los dominios de errores.
- Compruebe que los hosts de vSAN estén conectados. No es posible asignar hosts a un dominio de errores que está sin conexión o que no está disponible debido a un problema de configuración del hardware.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores**.
4. Haga clic en el icono más. Se abrirá el asistente Nuevo dominio de errores.
5. Introduzca el nombre del dominio de errores.
6. Seleccione un host o más para agregar al dominio de errores.

   Un dominio de errores no puede estar vacío. Debe seleccionar al menos un host para incluir en el dominio de errores.
7. Haga clic en **Crear**.

   Los hosts seleccionados se muestran en el dominio de errores. Cada dominio de errores muestra información de la capacidad utilizada y reservada. Esto permite ver la distribución de la capacidad en el dominio de errores.

Transferir hosts al dominio de errores seleccionado

Puede transferir un host a un dominio de errores seleccionado en el clúster de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores**.
4. Seleccione y arrastre el host que desea agregar a un dominio de errores existente.

   El host seleccionado aparecen en el dominio de errores.

Transferir hosts fuera de un dominio de errores

Según sus requisitos, puede transferir hosts fuera del dominio de errores.

Requisitos previos

Compruebe que el host esté en línea. No puede mover hosts que están sin conexión o no están disponibles en un dominio de errores.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

Opción	Descripción
vSphere Client	a Seleccione y arrastre el host desde el dominio de errores hacia el área Hosts independientes. b Haga clic en **Mover** para confirmar.
vSphere Web Client	a Seleccione el host que desea transferir y haga clic en el icono **Transferir hosts fuera del dominio de errores**. b Haga clic en **Yes** (Sí).

Resultados

El host seleccionado ya no forma parte del dominio de errores. Cualquier host que no forma parte de un dominio de errores se considera su propio dominio de errores de host individual.

Pasos siguientes

Puede agregar hosts a dominios de errores. Consulte Transferir hosts al dominio de errores seleccionado.

Cambiar el nombre de un dominio de errores

Puede cambiar el nombre de un dominio de errores existente en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

Opción	Descripción
vSphere Client	a Haga clic en el icono Acciones en el lado derecho del dominio de errores y seleccione **Editar**. b Introduzca un nombre de dominio de errores.
vSphere Web Client	a Seleccione el dominio de errores y haga clic en el icono **Cambiar nombre de dominio de errores seleccionado**. b Introduzca un nombre de dominio de errores.

4 Haga clic en **Aplicar** o en **Aceptar**.

El nombre nuevo aparecerá en la lista de dominios de errores.

Quitar dominios de errores seleccionados

Cuando ya no necesita un dominio de errores, puede quitarlo del clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

Opción	Descripción
vSphere Client	a Haga clic en el icono Acciones en el lado derecho del dominio de errores y seleccione **Eliminar**. b Haga clic en **Eliminar** para confirmar.
vSphere Web Client	a Seleccione el dominio de errores cuyo nombre desea eliminar y haga clic en el icono **Remove selected fault domains** (Quitar dominios de errores seleccionados) (❌). b Haga clic en **Yes** (Sí) para confirmar.

Resultados

Se quitan todos los hosts del dominio de errores y se elimina el dominio de errores seleccionado del clúster de vSAN. Se considera que cada host que no forma parte de un dominio de errores reside en su propio dominio de errores de host individual.

Usar el servicio del destino iSCSI de vSAN

Use el servicio del destino iSCSI para habilitar los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN para acceder al almacén de datos de vSAN.

Esta característica permite que un iniciador iSCSI en un host remoto transporte datos a nivel de bloque a un destino iSCSI en un dispositivo de almacenamiento del clúster de vSAN. vSAN 6.7 y las versiones posteriores admiten los clústeres de conmutación por error de Windows Server (WSFC), de modo que los nodos de WSFC pueden acceder a destinos de iSCSI de vSAN.

Tras configurar el servicio del destino iSCSI de vSAN, podrá detectar los destinos iSCSI de vSAN desde un host remoto. Para detectar destinos iSCSI de vSAN, use el puerto TCP del destino iSCSI y la dirección IP de cualquier host del clúster de vSAN. Para garantizar la alta disponibilidad del destino iSCSI de vSAN, configure el soporte de múltiples rutas para la aplicación iSCSI. Puede usar las direcciones IP de dos o más hosts para configurar múltiples rutas.

Nota El servicio del destino iSCSI de vSAN no admite otros clientes o iniciadores de vSphere o ESXi, hipervisores de terceros ni migraciones mediante asignaciones de dispositivos sin formato (Raw Device Mapping, RDM).

El servicio del destino iSCSI de vSAN admite los siguientes métodos de autenticación de CHAP:

CHAP

En la autenticación de CHAP, el destino autentica el iniciador, pero el iniciador no autentica el destino.

CHAP mutuo

En la autenticación de CHAP mutuo, un nivel extra de seguridad permite que el iniciador autentique el destino.

Para obtener más información sobre el uso del servicio del destino iSCSI de vSAN, consulte la guía de uso del destino iSCSI.

Destinos iSCSI

Puede agregar uno o más destinos iSCSI que proporcionen bloques de almacenamiento como números de unidad lógica (logical unit number, LUN). vSAN identifica cada destino iSCSI con un nombre completo de iSCSI (iSCSI qualified Name, IQN) único. Puede usar el IQN para presentar el destino iSCSI a un iniciador iSCSI remoto de modo que este pueda acceder al LUN del destino.

Cada destino iSCSI contiene uno o más LUN. En un clúster de vSAN se define el tamaño de cada LUN, se asigna una directiva de almacenamiento de vSAN a cada LUN y se habilita el servicio del destino iSCSI. Puede configurar una directiva de almacenamiento para usarla como directiva predeterminada del objeto de inicio del servicio del destino iSCSI de vSAN.

Grupos de iniciadores iSCSI

Puede definir un grupo de iniciadores iSCSI que tengan acceso a un destino iSCSI concreto. El grupo de iniciadores iSCSI solo permitirá el acceso de aquellos iniciadores que sean miembros del grupo. Si no define un iniciador o un grupo de iniciadores iSCSI, los iniciadores iSCSI podrán acceder a todos los destinos.

Un nombre único identifica a cada grupo de iniciadores iSCSI. Puede agregar uno o más iniciadores iSCSI como miembros del grupo. Use el IQN del iniciador como nombre del iniciador del miembro.

Habilitar el servicio del destino iSCSI

Antes de crear destinos y LUN iSCSI y definir grupos de iniciadores iSCSI, debe habilitar el servicio del destino iSCSI en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, haga clic en **Servicio del destino iSCSI**. b Haga clic para **Habilitar** el servicio de destino iSCSI de vSAN. c Edite la configuración del servicio de destino iSCSI de vSAN. Ahora es cuando se pueden seleccionar la red predeterminada, el puerto TCP y el método de autenticación. También puede seleccionar una directiva de almacenamiento de vSAN.
vSphere Web Client	a En vSAN, haga clic en **Destinos iSCSI**. b Haga clic en el botón **Editar** del servicio de destino iSCSI de vSAN. c Seleccione la casilla Habilitar el servicio de destino iSCSI de vSAN. Ahora es cuando se pueden seleccionar la red predeterminada, el puerto TCP y el método de autenticación. También puede seleccionar una directiva de almacenamiento de vSAN.

3 Haga clic en **Aceptar** o en **Aplicar**.

Pasos siguientes

Tras habilitar el servicio del destino iSCSI, podrá crear destinos y LUN iSCSI, así como definir grupos de iniciadores iSCSI.

Crear un destino iSCSI

Puede crear o editar un destino iSCSI y su LUN asociado.

Requisitos previos

Compruebe que el servicio del destino iSCSI esté habilitado.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, haga clic en **Servicio del destino iSCSI**. b Haga clic en la pestaña Destinos iSCSI. c Haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Nuevo destino iSCSI**. Si deja en blanco el campo IQN de destino, se genera automáticamente el IQN. d Escriba un alias para el destino. También puede editar la red, el puerto TCP y el método de autenticación del destino.
vSphere Web Client	a En vSAN, haga clic en **Destinos iSCSI**. b En la sección Destinos iSCSI de vSAN, haga clic en el icono **Agregar un nuevo destino iSCSI**. Se abrirá el cuadro de diálogo Nuevo destino iSCSI. El IQN del destino se generará de forma automática. c Escriba un alias para el destino. También puede editar la red, el puerto TCP y el método de autenticación del destino. d (Opcional) Para definir el LUN de destino, haga clic en la casilla Agregar el primer LUN al destino iSCSI e introduzca el tamaño del LUN.

3 Haga clic en **Aceptar**.

Pasos siguientes

Defina la lista de iniciadores iSCSI que podrán acceder a este destino.

Agregar un LUN a un destino iSCSI

Puede agregar uno o más LUN a un destino iSCSI, o editar un LUN existente.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, haga clic en **Servicio del destino iSCSI**. b Haga clic en la pestaña Destinos iSCSI y seleccione un destino. c En la sección de LUN de iSCSI de vSAN, haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Agregar LUN al destino**. d Introduzca el tamaño del LUN. La directiva de almacenamiento de vSAN configurada para el servicio del destino iSCSI se asignará de forma automática. Puede asignar otra directiva a los LUN.
vSphere Web Client	a En vSAN, haga clic en **Destinos iSCSI**. b Seleccione un destino y la pestaña LUN en la sección Detalles del destino de la página. c Haga clic en el icono **Agregar nuevo LUN iSCSI al destino**. Se abrirá el cuadro de diálogo Agregar LUN al destino. d Introduzca el tamaño del LUN. Se asignará de forma automática la directiva de almacenamiento de vSAN configurada para el servicio del destino iSCSI. Puede asignar otra directiva a los LUN.

3 Haga clic en **Agregar**.

Cambiar el tamaño de un LUN en un destino iSCSI

En función de sus requisitos, puede aumentar el tamaño de un LUN en línea. El cambio de tamaño en línea del LUN se habilita solo si todos los hosts del clúster se actualizan a vSAN 6.7 Update 3 o una versión posterior.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Servicio del destino iSCSI**.

4 Haga clic en la pestaña **Destinos iSCSI** y seleccione un destino.

5 En la sección LUN iSCSI de vSAN, seleccione un LUN y haga clic en **Editar**. Aparece el cuadro de dialogo de Editar LUN.

6 Aumente el tamaño del LUN en función de sus requisitos.

7 Haga clic en **OK** (Aceptar).

Crear un grupo de iniciadores iSCSI

Puede crear un grupo de iniciadores iSCSI para conceder control de acceso a los destinos iSCSI. Solo los iniciadores iSCSI que sean miembros del grupo de iniciadores podrán acceder a los destinos iSCSI.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, haga clic en **Servicio del destino iSCSI**. b Haga clic en la pestaña Grupos de iniciadores y seleccione el icono **Agregar un nuevo grupo de iniciadores iSCSI** (+). Aparecerá el cuadro de diálogo **Nuevo grupo de iniciadores**. c Escriba un nombre para el grupo de iniciadores iSCSI. d (Opcional) Para agregar miembros al grupo de iniciadores, escriba el IQN de cada miembro. Use el siguiente formato para introducir el IQN de los miembros: *iqn.YYYY-MM.domain:name* Donde: ■ YYYY = año, como 2016 ■ MM = mes, como 09 ■ domain = dominio donde se encuentra el iniciador ■ name = nombre del miembro (opcional)
vSphere Web Client	a En vSAN, haga clic en **Grupos de iniciadores iSCSI**. b En la sección Grupos de iniciadores iSCSI de vSAN, haga clic en el icono **Agregar un nuevo grupo de iniciadores iSCSI**. Se mostrará el cuadro de diálogo Nuevo grupo de iniciadores iSCSI de vSAN. c Escriba un nombre para el grupo de iniciadores iSCSI. d (Opcional) Para agregar miembros al grupo de iniciadores, escriba el IQN de cada miembro. Use el siguiente formato para introducir el IQN de los miembros: *iqn.YYYY-MM.domain:name* Donde: ■ YYYY = año, como 2016 ■ MM = mes, como 09 ■ domain = dominio donde se encuentra el iniciador ■ name = nombre del miembro (opcional)

3 Haga clic en **Aceptar** o **Crear**.

Pasos siguientes

Agregue miembros al grupo de iniciadores iSCSI.

Asignar un destino a un grupo de iniciadores iSCSI

Puede asignar un destino iSCSI a un grupo de iniciadores iSCSI. Solo los iniciadores que sean miembros del grupo de iniciadores podrán acceder a los destinos asignados.

Requisitos previos

Compruebe que haya un grupo de iniciadores iSCSI.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, haga clic en **Servicio del destino iSCSI**. b Seleccione la pestaña **Grupos de iniciadores**. c En la sección Destinos accesibles, haga clic en el icono **Agregar un nuevo destino accesible para el grupo de iniciadores iSCSI** (). Se mostrará el cuadro de diálogo **Agregar destinos accesibles**. d Seleccione un destino de la lista de destinos accesibles.
vSphere Web Client	a En vSAN, haga clic en **Destinos iSCSI**. b Seleccione la pestaña Grupos de iniciadores. c En la sección Detalles del grupo, seleccione la pestaña Destinos accesibles. d Haga clic en el icono **Agregar un nuevo destino accesible para el grupo de iniciadores iSCSI**. Se mostrará el cuadro de diálogo Agregar destinos accesibles. e En la pestaña Filtro, seleccione un destino de la lista de destinos disponibles. La pestaña Objetos seleccionados mostrará los destinos seleccionados actualmente.

3 Haga clic en **Agregar**.

Supervisar el servicio del destino iSCSI de vSAN

Puede supervisar el servicio del destino iSCSI para ver la colocación física de los componentes del destino iSCSI, así como para comprobar los componentes con errores. También puede supervisar el estado de mantenimiento del servicio del destino iSCSI.

Requisitos previos

Compruebe que se haya habilitado el servicio del destino iSCSI de vSAN y que se hayan creado los destinos y los LUN.

Procedimiento

◆ Desplácese hasta el clúster de vSAN.

Opción	Descripción
vSphere Client	a Haga clic en **Supervisar** y, a continuación, seleccione **Objetos virtuales**. Los destinos iSCSI se enumeran en la página. b Seleccione un destino y haga clic en **Ver detalles de colocación**. La colocación física muestra el lugar donde se encuentran los componentes de datos del destino. c Haga clic en **Agrupar componentes por colocación de hosts** para ver los hosts asociados con los componentes de datos iSCSI.
vSphere Web Client	a Haga clic en **Supervisar** y seleccione **vSAN**. b Haga clic en **Destinos iSCSI**. Los destinos y los LUN iSCSI aparecerán en la parte superior de la página. c Haga clic en un alias de destino para ver su estado. La pestaña Colocación de discos físicos de la parte inferior de la página muestra el lugar donde se encuentran los componentes de datos del destino. La pestaña Errores de cumplimiento muestra los componentes con errores. d Haga clic en un LUN para ver su estado. La pestaña Colocación de discos físicos de la parte inferior de la página muestra el lugar donde se encuentran los componentes de datos del LUN. La pestaña Errores de cumplimiento muestra los componentes con errores.

Migrar un clúster híbrido de vSAN a un clúster basado íntegramente en tecnología flash

Puede migrar los grupos de discos de un clúster híbrido de vSAN a grupos de discos basados íntegramente en tecnología flash.

El clúster híbrido de vSAN usa discos magnéticos para la capa de capacidad, y dispositivos flash para la capa de memoria caché. Puede cambiar la configuración de los grupos de discos del clúster de modo que se usen dispositivos flash en la capa de memoria caché y la capa de capacidad.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Quite los grupos de discos híbridos de los hosts del clúster.

   a Haga clic en la pestaña **Configurar**.

   b En vSAN, haga clic en **Administración de discos**.

   c En Grupos de discos, seleccione el grupo de discos que desea eliminar, haga clic en **...** y, a continuación, en **Quitar**.

   d Seleccione **Migración de datos completa** como modo de migración y haga clic en **Sí**.

3 Quite los discos HDD físicos del host.

4 Agregue los dispositivos flash al host.

   Compruebe que no haya particiones en los dispositivos flash.

5 Cree los grupos de discos basados íntegramente en tecnología flash en los hosts.

Apagar y reiniciar manualmente el clúster de vSAN

Puede apagar manualmente todo el clúster de vSAN para realizar tareas de mantenimiento o solucionar problemas.

Utilice el asistente Apagar clúster a no ser que el flujo de trabajo requiera un apagado manual. Cuando apague manualmente el clúster de vSAN, no deshabilite vSAN en el clúster.

Nota Si tiene un entorno de vSphere with Tanzu, debe seguir el orden especificado al apagar o iniciar los componentes. Para obtener más información, consulte "Apagar e iniciar VMware Cloud Foundation" en la *Guía de operaciones de VMware Cloud Foundation*.

Procedimiento

1 Apague el clúster de vSAN.

   a Compruebe el servicio de estado de vSAN para confirmar que el clúster está en buen estado.

   b Apague todas las máquinas virtuales que se ejecutan en el clúster de vSAN si vCenter Server no está alojado en el clúster. Si vCenter Server está alojado en el clúster de vSAN, no apague la máquina virtual de vCenter Server.

   c Haga clic en la pestaña **Configurar** y desactive HA. Como resultado, el clúster no registrará apagados de hosts como errores.

      Para vSphere 7.0 U1 y versiones posteriores, habilite el modo de retirada de vCLS. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/80472.

   d Compruebe que todas las tareas de resincronización se hayan completado.

      Haga clic en la pestaña **Supervisar** y seleccione **vSAN** > **Resincronización de objetos**.

   e Si vCenter Server está alojado en el clúster de vSAN, apague la máquina virtual de vCenter Server.

      Tome nota del host que ejecuta la máquina virtual vCenter Server. Es el host en el que se debe reiniciar la máquina virtual de vCenter Server.

   f Deshabilite las actualizaciones de los miembros del clúster desde vCenter Server ejecutando el siguiente comando en los hosts de ESXi del clúster. Asegúrese de ejecutar el siguiente comando en todos los hosts.

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

   g Inicie sesión en cualquier host del clúster que no sea el host testigo.

h Ejecute el siguiente comando solo en ese host. Si ejecuta el comando en varios hosts a la vez, puede provocar que una condición de carrera cause resultados inesperados.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

El comando devuelve e imprime lo siguiente:

`Se realizó la preparación del clúster.`

Nota

- El clúster está totalmente particionado después de que el comando se haya completado correctamente.
- Si se produce un error, solucione el problema en función del mensaje de error y vuelva a habilitar el modo de retirada de vCLS.
- Si hay hosts desconectados o en mal estado en el clúster, elimine los hosts y vuelva a intentar ejecutar el comando.

---

i Coloque todos los hosts en modo de mantenimiento con **Sin acción**. Si vCenter Server está apagado, use el siguiente comando para colocar los hosts de ESXi en el modo de mantenimiento con **Sin acción**.

```
esxcli system maintenanceMode set -e true -m noAction
```

Realice este paso en todos los hosts.

Para evitar el riesgo de falta de disponibilidad de datos al utilizar **Sin acción** al mismo tiempo en varios hosts, y después de reiniciar varios hosts, consulte este artículo de la base de conocimientos de VMware: https://kb.vmware.com/s/article/60424. Para realizar un reinicio simultáneo de todos los hosts del clúster mediante una herramienta integrada, consulte este artículo de la base de conocimientos de VMware: https://kb.vmware.com/s/article/70650.

j Después de que todos los hosts hayan entrado correctamente en el modo de mantenimiento, realice las tareas de mantenimiento necesarias y apague los hosts.

2 Reinicie el clúster de vSAN.

a Encienda los hosts ESXi.

Encienda el cuadro físico en el que está instalado ESXi. El host de ESXi se inicia, busca las máquinas virtuales correspondientes y funciona con normalidad.

Si algún host no se reinician, deberá recuperarlo de forma manual o moverlo fuera del clúster de vSAN.

b Cuando todos los hosts vuelvan a encenderse, salga del modo de mantenimiento en todos los hosts. Si vCenter Server está apagado, use el siguiente comando en los hosts de ESXi para salir del modo de mantenimiento.

```
esxcli system maintenanceMode set -e false
```

Realice este paso en todos los hosts.

c Inicie sesión en uno de los hosts del clúster que no sean el host testigo.

d Ejecute el siguiente comando solo en ese host. Si ejecuta el comando en varios hosts a la vez, puede provocar que una condición de carrera cause resultados inesperados.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

El comando devuelve e imprime lo siguiente:

`El reinicio o encendido del clúster se completó correctamente.`

e Compruebe que todos los hosts estén disponibles en el clúster ejecutando el siguiente comando en cada host.

```
esxcli vsan cluster get
```

f Habilite las actualizaciones de miembros del clúster desde vCenter Server ejecutando el siguiente comando en los hosts de ESXi del clúster. Asegúrese de ejecutar el siguiente comando en todos los hosts.

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

g Reinicie la máquina virtual de vCenter Server si está apagada. Espere a que la máquina virtual de vCenter Server se encienda y se ejecute. Para deshabilitar el modo de retirada de vCLS, consulte el artículo de la base de conocimiento de VMware en https://kb.vmware.com/s/article/80472.

h Compruebe que todos los hosts estén disponibles en el clúster de vSAN ejecutando el siguiente comando en cada host.

```
esxcli vsan cluster get
```

i Reinicie las máquinas virtuales restantes a través de vCenter Server.

j Compruebe el servicio de estado de vSAN y resuelva los problemas pendientes.

k (Opcional) Si el clúster de vSAN tiene habilitada Disponibilidad de vSphere, debe reiniciar manualmente Disponibilidad de vSphere para evitar el siguiente error: `No se puede encontrar el agente principal de vSphere HA`.

Para reiniciar de forma manual Disponibilidad de vSphere, seleccione el clúster de vSAN y acceda a:

1 **Configurar** > **Servicios** > **Disponibilidad de vSphere** > **EDITAR** > **Deshabilitar vSphere HA**

2 **Configurar** > **Servicios** > **Disponibilidad de vSphere** > **EDITAR** > **Habilitar vSphere HA**

3 Si hay hosts desconectados o en mal estado en el clúster, recupere o elimine los hosts del clúster de vSAN. Vuelva a intentar los comandos anteriores solo después de que el servicio de estado de vSAN muestre todos los hosts disponibles en estado verde.

Si tiene un clúster de vSAN de tres nodos, el comando `reboot_helper.py recover` no puede funcionar en una situación de error de un host. Como administrador, haga lo siguiente:

a Elimine temporalmente la información del host de error de la lista de agentes de unidifusión.

b Agregue el host después de ejecutar el siguiente comando.

```
reboot_helper.py recover
```

A continuación, se muestran los comandos para eliminar y agregar el host a un clúster de vSAN:

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p
12321
```

Apagar un clúster de vSAN

Puede apagar un clúster de vSAN para realizar tareas de mantenimiento o actualización.

Requisitos previos

Si la máquina virtual de vCenter Server se ejecuta en el clúster de vSAN, mígrela al primer host, o registre el host donde se ejecuta actualmente.

Procedimiento

1 Apague todas las máquinas virtuales que se ejecuten en el clúster de vSAN.

Si vCenter Server se ejecuta en el clúster de vSAN, la máquina virtual de vCenter Server debe apagarse en último lugar.

2 Coloque todos los hosts ESXi que formen parte del clúster en modo de mantenimiento.

   Consulte Poner un miembro de un clúster de vSAN en modo de mantenimiento

3 Apague los hosts ESXi.

Administrar dispositivos en un clúster de vSAN

5

Puede realizar varias tareas de administración de dispositivos en un clúster de vSAN. Puede crear grupos de discos híbridos o basados íntegramente en tecnología flash, habilitar vSAN para reclamar dispositivos para memoria caché y capacidad, habilitar o deshabilitar los indicadores LED en los dispositivos, marcar dispositivos como flash, marcar dispositivos remotos como locales, etc.

Este capítulo incluye los siguientes temas:

Administrar grupos de discos y dispositivos

Cuando habilite vSAN en un clúster, seleccione un modo de reclamación de discos para organizar los dispositivos en grupos.

vSAN 6.6 y las versiones posteriores cuentan con un flujo de trabajo uniforme para el reclamo de discos en todos los escenarios. Los discos disponibles se agrupan por modelo y tamaño o por host. Debe seleccionar los dispositivos que destinará para almacenamiento en caché y los que usará para capacidad.

Crear un grupo de discos en un host

Al crear grupos de discos, es necesario especificar cada host y cada dispositivo que se utilizarán para el almacén de datos de vSAN. Organice los dispositivos de almacenamiento en caché y de capacidad en grupos de discos.

Para crear un grupo de discos, debe definir el grupo de discos y seleccionar los dispositivos de forma individual para incluirlos en dicho grupo. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y uno o varios dispositivos de capacidad.

Cuando cree un grupo de discos, tenga en cuenta la proporción entre el almacenamiento en caché flash y la capacidad consumida. La proporción depende de los requisitos y de la carga de trabajo del clúster. En un clúster híbrido, considere utilizar al menos un 10 % de memoria caché flash para la proporción de capacidad utilizada (sin incluir réplicas, como duplicados).

El clúster de vSAN contiene inicialmente un solo almacén de datos de vSAN con cero bytes consumidos.

A medida que crea grupos de discos en cada host y agrega dispositivos de capacidad y memoria caché, el tamaño del almacén de datos aumenta en función de la cantidad de capacidad física que agregaron estos dispositivos. vSAN crea un solo almacén de datos distribuido de vSAN utilizando la capacidad local vacía que está disponible en los hosts agregados al clúster.

Cada grupo de discos incluye un solo dispositivo flash de almacenamiento en caché. Puede crear varios grupos de discos de forma manual y reclamar un dispositivo flash de almacenamiento en caché para cada grupo.

Nota Si se agrega un nuevo host ESXi al clúster de vSAN, el almacenamiento local de ese host no se agrega automáticamente al almacén de datos de vSAN. Debe crear un grupo de discos y agregar los dispositivos al grupo de discos para usar el nuevo almacenamiento del nuevo host de ESXi.

Reclamar discos para el clúster de vSAN

Puede seleccionar varios dispositivos de los hosts. vSAN crea grupos de discos predeterminados por usted.

Cuando agrega más capacidad a los hosts o añade nuevos hosts con capacidad, puede seleccionar los dispositivos nuevos para incrementar la capacidad del almacén de datos de vSAN. En un clúster basado íntegramente en tecnología flash, puede marcar los dispositivos flash para usarlos como capacidad.

Después de que vSAN haya reclamado dispositivos, crea el almacén de datos compartidos de vSAN. El tamaño total del almacén de datos refleja la capacidad de todos los dispositivos de capacidad en los grupos de discos de todos los hosts en el clúster. Para los metadatos, se utilizan algunas sobrecargas de capacidad.

Crear un grupo de discos en un host de vSAN

Puede combinar manualmente dispositivos específicos de almacenamiento en caché y ciertos dispositivos de capacidad para definir grupos de discos en un host en particular.

Con este método, debe seleccionar dispositivos manualmente para crear un grupo de discos para un host. Debe agregar un dispositivo de almacenamiento en caché y, al menos, un dispositivo de capacidad al grupo de discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, haga clic en **Disk Management** (Administración de discos).
4 Seleccione el host y haga clic en **Crear grupo de discos**.
   - Seleccione el dispositivo flash que se utilizará para el almacenamiento en caché.

- Seleccione el tipo de discos de capacidad que desea utilizar según el tipo de grupo de discos que desea crear (HDD para elementos híbridos, o bien Flash para elementos basados en flash).
- Seleccione los dispositivos que desea utilizar para capacidad.

5 Haga clic en **Crear** o en **Aceptar** para confirmar su selección.

Resultados

El nuevo grupo de discos se muestra en la lista.

Reclamar dispositivos de almacenamiento para un clúster de vSAN

Puede seleccionar un grupo de dispositivos de capacidad y de memoria caché. vSAN los organizará en grupos de discos predeterminados.

Procedimiento

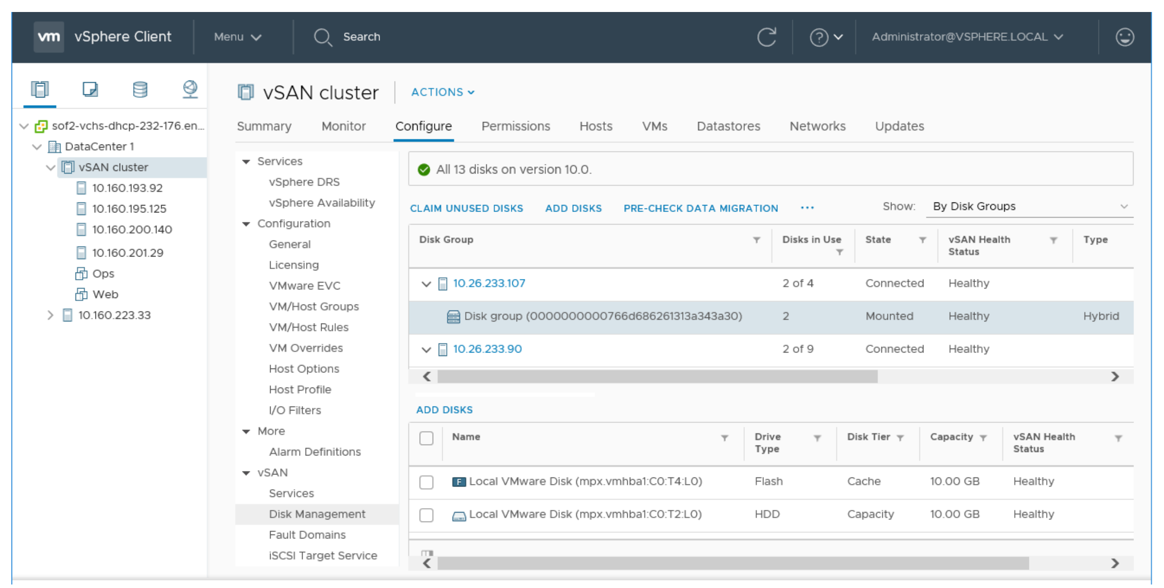
1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Disk Management** (Administración de discos).
4. Haga clic en **Reclamar discos sin utilizar**.
5. Seleccione los dispositivos que se agregarán al grupo de discos.
   - Para los grupos de discos híbridos, cada host que aporta almacenamiento debe aportar un dispositivo flash de memoria caché, así como uno o varios dispositivos de capacidad HDD. Puede agregar un solo dispositivo de memoria caché por grupo de discos.
     - Seleccione un dispositivo flash que se utilizará como memoria caché y haga clic en **Reclamar por nivel de memoria caché**.
     - Seleccione el dispositivo HDD que se utilizará como capacidad y haga clic en **Reclamar por nivel de capacidad**.
     - Haga clic en **Crear** o en **Aceptar**.
   - Para los grupos de discos basados en flash, cada host que aporta almacenamiento debe aportar un dispositivo flash de memoria caché, así como uno o varios dispositivos de capacidad flash. Puede agregar un solo dispositivo de memoria caché por grupo de discos.
     - Seleccione un dispositivo flash que se utilizará como memoria caché y haga clic en **Reclamar por nivel de memoria caché**.
     - Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en **Reclamar por nivel de capacidad**.
     - Haga clic en **Crear** o en **Aceptar**.

Para comprobar la función de cada dispositivo agregado al grupo de discos basado íntegramente en tecnología flash, desplácese hasta la columna Disk Role (Función de disco) en la parte inferior de la página Disk Management (Administración de discos). La columna muestra la lista de dispositivos y su función en un grupo de discos.

vSAN reclama los dispositivos seleccionados y los organiza en grupos de discos predeterminados que respaldan el almacén de datos de vSAN.

Trabajar con dispositivos individuales

Puede realizar varias tareas de administración de dispositivos en el clúster de vSAN, como agregar dispositivos a un grupo de discos, eliminar dispositivos de un grupo de discos, habilitar o deshabilitar los LED del localizador y marcar dispositivos.



Agregar dispositivos al grupo de discos

Cuando configura vSAN para reclamar discos en modo manual, puede agregar dispositivos locales adicionales a los grupos de discos existentes.

Los dispositivos deben ser del mismo tipo que los dispositivos existentes en los grupos de discos, como discos de estado sólido (SSD) o discos magnéticos.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione el grupo de discos y haga clic en **Agregar discos**.

5 Seleccione el dispositivo que desea agregar y haga clic en **Agregar**.

Si agrega un dispositivo usado que contiene información de particiones o datos residuales, en primer lugar debe limpiar el dispositivo. Si desea conocer el procedimiento para quitar información de particiones de los dispositivos, consulte Quitar particiones de dispositivos. También es posible ejecutar el comando de RVC `host_wipe_vsan_disks` para aplicar formato al dispositivo. Para obtener más información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Pasos siguientes

Verifique que la comprobación de estado del equilibrio de disco de vSAN sea de color verde. Si la comprobación de estado del equilibrio de disco emite una advertencia, ejecute una operación de redistribución manual fuera de las horas punta. Para obtener más información, consulte "Redistribución manual" en *Supervisar vSAN y solucionar sus problemas*.

Quitar grupos de discos o dispositivos de vSAN

Puede quitar dispositivos seleccionados del grupo de discos o un grupo de discos completo.

Dado que quitar dispositivos no protegidos puede ser un proceso disruptivo para el almacén de datos de vSAN y las máquinas virtuales del almacén de datos, evite quitar dispositivos o grupos de discos.

Por lo general, se quitan dispositivos o grupos de discos de vSAN cuando se actualiza un dispositivo o se reemplaza un dispositivo con errores, o cuando se debe quitar un dispositivo de memoria caché. Otras características de almacenamiento de vSphere pueden usar cualquier dispositivo basado en flash que se quite del clúster de vSAN.

La eliminación permanente de un grupo de discos elimina los miembros del disco y los datos almacenados en los dispositivos.

Nota Al quitar un dispositivo flash de almacenamiento en caché o todos los dispositivos de capacidad de un grupo de discos, se quita el grupo de discos completo.

La evacuación de datos de dispositivos o grupos de discos puede ocasionar un incumplimiento temporal de las directivas de almacenamiento de máquinas virtuales.

Requisitos previos

- Si desea poner el host de vSAN en modo de mantenimiento, seleccione la opción **Migración de datos completa** o la opción **Garantizar accesibilidad a los datos** al eliminar un dispositivo o un grupo de discos. Si selecciona **No data migration** (Sin migración de datos) desde el menú desplegable, es posible que los datos estén en riesgo si ocurre un error durante la evacuación.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Disk Management** (Administración de discos).

4 Quite el grupo de discos o los dispositivos seleccionados.

Opción	Descripción
Remove the Disk Group (Quitar el grupo de discos)	a En Grupos de discos, seleccione el grupo de discos que desea eliminar, haga clic en **...** y, a continuación, haga clic en **Quitar**. b Seleccione un modo de evacuación de datos.
Remove the Selected Device (Quitar el dispositivo seleccionado)	a En Disk Groups (Grupos de discos), seleccione el grupo de discos que contiene el dispositivo que desea quitar. b En Discos, seleccione el dispositivo que desea eliminar y haga clic en el icono **Quitar discos**. c Seleccione un modo de evacuación de datos.

Puede transferir los datos evacuados a otro disco u otro grupo de discos del mismo host.

5 Haga clic en **Sí** o en **Quitar** para confirmar.

Los datos se evacúan de los dispositivos seleccionados o de un grupo de discos, y dejan de estar disponibles en vSAN.

Volver a crear un grupo de discos

Cuando se vuelve a crear un grupo de discos en el clúster de vSAN, los discos existentes se quitan del grupo de discos y este se elimina. vSAN vuelve a crear el grupo de discos con los mismos discos.

Cuando se vuelve a crear un grupo de discos en un clúster de vSAN, vSAN administra el proceso por usted. vSAN evacua los datos de todos los discos en el grupo de discos, quita el grupo de discos y crea el grupo de discos con los mismos discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Disk Management** (Administración de discos).

4 En Grupos de discos, seleccione el grupo de discos que desea volver a crear.

5 Haga clic en **...** y, a continuación, haga clic en **Volver a crear**.

Aparece el cuadro de diálogo Volver a crear grupo de discos.

6 Seleccione un modo de migración de datos y haga clic en **Volver a crear**.

Resultados

Se evacuan todos los datos que residen en los discos. El grupo de discos se elimina del clúster y se vuelve a crear.

Usar los LED del localizador

No puede usar los LED del localizador para identificar la ubicación de los dispositivos de almacenamiento.

vSAN puede encender el LED del localizador en un dispositivo con errores a fin de que pueda identificar fácilmente el dispositivo. Esto resulta especialmente útil al trabajar con varios escenarios de conexión e intercambio en caliente.

Considere utilizar controladoras de almacenamiento de E/S con el modo de paso, debido a que las controladoras con el modo RAID 0 requieren pasos adicionales para habilitar el reconocimiento de las controladoras de los LED del localizador.

Para obtener información sobre la configuración de las controladoras de almacenamiento en modo RAID 0, consulte la documentación del proveedor.

Habilitar y deshabilitar los LED del localizador

Puede activar o desactivar los LED del localizador de los dispositivos de almacenamiento de vSAN. Cuando active el LED del localizador, puede identificar la ubicación de un dispositivo de almacenamiento específico.

Cuando ya no necesite una alerta visual de los dispositivos de vSAN, puede desactivar los LED del localizador en los dispositivos seleccionados.

Requisitos previos

- Compruebe que haya instalado los controladores compatibles para las controladoras de E/S de almacenamiento que habilitan esta característica. Para obtener información sobre los controladores que están certificados por VMware, consulte la *Guía de compatibilidad de VMware* en la URL: http://www.vmware.com/resources/compatibility/search.php.
- En algunos casos, es posible que necesite usar utilidades de otros fabricantes para configurar la característica de los LED del localizador en las controladoras de E/S de almacenamiento. Por ejemplo, al usar HP, debe comprobar que esté instalada la CLI de HP SSA.

Para obtener más información sobre la instalación de VIB de otros fabricantes, consulte el documento *Actualización de vSphere*.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione un host para ver la lista de dispositivos.

5 En la parte inferior de la página, seleccione un dispositivo de almacenamiento o más de la lista, y habilite o deshabilite los LED del localizador en los dispositivos seleccionados.

Opción	Acción
Encender LED	Habilita el LED del localizador en el dispositivo de almacenamiento seleccionado. Los LED del localizador se pueden habilitar desde la pestaña **Manage** (Administrar) y haciendo clic en **Storage** (Almacenamiento) **> Storage Devices** (Dispositivos de almacenamiento).
Apagar LED	Deshabilita el LED del localizador en el dispositivo de almacenamiento seleccionado. Los LED del localizador se pueden deshabilitar desde la pestaña **Manage** (Administrar) y haciendo clic en **Storage** (Almacenamiento) **> Storage Devices** (Dispositivos de almacenamiento).

Marcar dispositivos como dispositivos flash

Cuando los hosts ESXi no identifican automáticamente los dispositivos flash como tales, puede marcarlos manualmente como dispositivos flash locales.

Es posible que los dispositivos flash no se reconozcan como flash cuando admiten el modo RAID 0 en lugar del modo de acceso directo. Cuando los dispositivos no se reconocen como dispositivos flash locales, se excluyen de la lista de dispositivos que se ofrecen para vSAN y no es posible utilizarlos en el clúster de vSAN. Cuando estos dispositivos se marcan como dispositivos flash locales, pasan a estar disponibles para vSAN.

Requisitos previos

- Compruebe que el dispositivo sea local para el host.
- Compruebe que el dispositivo no esté en uso.
- Asegúrese de que las máquinas virtuales que acceden al dispositivo estén apagadas y de que el almacén de datos esté desmontado.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Disk Management** (Administración de discos).

4 Seleccione el host para ver la lista de dispositivos disponibles.

5 Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).

6 Seleccione uno o varios dispositivos flash de la lista y haga clic en **Marcar como disco flash**.

7 Haga clic en **Yes** (Sí) para guardar los cambios.

El tipo de unidad de los dispositivos seleccionados aparecerá como Flash.

Marcar dispositivos como discos HDD

Cuando los hosts ESXi no identifican automáticamente los discos magnéticos locales como dispositivos HDD, puede marcarlos manualmente como dispositivos HDD locales.

Si ha marcado un disco magnético como dispositivo flash, puede cambiar el tipo de disco del dispositivo marcándolo como disco magnético.

Requisitos previos

- Compruebe que el disco magnético sea local para el host.
- Compruebe que el disco magnético no esté en uso y que esté vacío.
- Compruebe que las máquinas virtuales que acceden al dispositivo estén apagadas.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione el host para ver la lista de dispositivos magnéticos disponibles.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).
6. Seleccione uno o varios discos magnéticos en la lista y haga clic en **Marcar como disco HDD**.
7. Haga clic en **Yes** (Sí) para guardar.

   El tipo de unidad de los discos magnéticos seleccionados aparece como HDD.

Marcar dispositivos como locales

Cuando los hosts usan gabinetes SAS externos, es posible que vSAN reconozca ciertos dispositivos como remotos y que no pueda reclamarlos de manera automática como locales.

En dichos casos, puede indicar que los dispositivos son locales.

Requisitos previos

Asegúrese de que el dispositivo de almacenamiento no sea un dispositivo compartido.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione un host para ver la lista de dispositivos.
5. Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).

6 En la lista de dispositivos, seleccione el o los dispositivos remotos que desee marcar como locales y haga clic en **Marcar como disco local**.

7 Haga clic en **Yes** (Sí) para guardar los cambios.

Marcar dispositivos como remotos

Los hosts que usan controladores SAS externos pueden compartir dispositivos. Esos dispositivos compartidos pueden marcarse manualmente como remotos, de modo que vSAN no reclame los dispositivos al crear grupos de discos.

En vSAN, no es posible agregar dispositivos compartidos a un grupo de discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un host para ver la lista de dispositivos.

5 Desde el menú desplegable **Show** (Mostrar), ubicado en la parte inferior de la página, seleccione **Not in Use** (No en uso).

6 Seleccione el o los dispositivos que desee marcar como remotos y haga clic en **Marcar como remoto**.

7 Haga clic en **Yes** (Sí) para confirmar.

Agregar un dispositivo de capacidad

Es posible agregar un dispositivo de capacidad a un grupo de discos de vSAN existente.

No es posible agregar dispositivos compartidos a un grupo de discos.

Requisitos previos

Compruebe que el dispositivo no tenga formato y no esté en uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un grupo de discos.

5 Haga clic en **Agregar discos** en la parte inferior de la página.

6 Seleccione el dispositivo de capacidad que desea agregar al grupo de discos.

7 Haga clic en **Aceptar** o en **Agregar**.

   El dispositivo se agregará al grupo de discos.

Quitar particiones de dispositivos

Puede quitar la información de particiones de un dispositivo a fin de que vSAN pueda reclamar el dispositivo y utilizarlo.

Si ha agregado un dispositivo que contiene información de particiones o datos residuales, debe quitar toda la información de particiones previa del dispositivo antes de reclamarlo para utilizarlo con vSAN. VMware recomienda agregar dispositivos limpios a los grupos de discos.

Al quitar información de particiones de un dispositivo, vSAN elimina la partición principal que incluye la información de formato del disco y las particiones lógicas del dispositivo.

Requisitos previos

Compruebe que ESXi no esté utilizando el dispositivo como disco de arranque, almacén de datos de VMFS o vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un host para ver la lista de dispositivos disponibles.

5 En el menú desplegable **Mostrar**, seleccione **No válidos**.

6 Seleccione un dispositivo de la lista.

Opción	Descripción
vSphere Client	Haga clic en **Borrar particiones**.
vSphere Web Client	Haga clic en el icono **Borrar particiones** ( ).

7 Haga clic en **OK** (Aceptar) para confirmar.

El dispositivo se encuentra limpio y no contiene información de particiones.

Aumentar la eficiencia de espacio en un clúster de vSAN

6

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos. Estas técnicas reducen el espacio de almacenamiento total requerido para satisfacer sus necesidades.

Este capítulo incluye los siguientes temas:

Introducción a la eficiencia de espacio de vSAN

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos. Estas técnicas reducen la capacidad de almacenamiento total requerida para satisfacer sus necesidades.

vSAN 6.7 Update 1 y las versiones posteriores admiten comandos de anulación de asignaciones SCSI que permiten reclamar espacio de almacenamiento asignado a un objeto de vSAN eliminado.

Puede habilitar la desduplicación y la compresión en un clúster de vSAN para eliminar los datos duplicados y reducir la cantidad de espacio necesario para almacenar datos.

Puede establecer el atributo de la directiva **Failure tolerance method** (Método de tolerancia ante errores) para utilizar la codificación de borrado RAID 5 o RAID 6. La codificación de borrado puede proteger sus datos y, al mismo tiempo, utilizar menos espacio de almacenamiento que el método de reflejo RAID 1 predeterminado.

Puede utilizar la desduplicación y compresión, y la codificación de borrado RAID 5 o RAID 6 para aumentar los ahorros en espacio de almacenamiento. RAID 5 o RAID 6 proporcionan ahorros de espacio claramente definidos en comparación con RAID 1. La desduplicación y la compresión pueden proporcionar ahorros adicionales.

Reclamar espacio con la anulación de asignación de SCSI

vSAN 6.7 Update 1 y las versiones posteriores admiten comandos UNMAP de SCSI que permiten recuperar espacio de almacenamiento asignado a un objeto de vSAN eliminado.

Al eliminar o quitar los archivos, se libera espacio en el sistema de archivos. Este espacio libre queda asignado a un dispositivo de almacenamiento hasta que el sistema de archivos lo libera o anula la asignación. vSAN admite la recuperación de espacio libre, también denominada operación de anulación de asignación. Puede liberar espacio de almacenamiento dentro del almacén de datos de vSAN al eliminar o migrar una máquina virtual o al consolidar una instantánea, entre otras acciones.

La recuperación de espacio de almacenamiento puede proporcionar mayor capacidad de proceso de E/S de flash a host y mejorar la resistencia de flash.

vSAN también admite los comandos UNMAP de SCSI emitidos directamente desde un sistema operativo invitado para recuperar espacio de almacenamiento. vSAN es compatible con asignaciones tanto fuera de línea como en línea. En el sistema operativo Linux, las anulaciones de asignación sin conexión se llevan a cabo con el comando **`fstrim(8)`**, y las anulaciones de asignación en línea se llevan a cabo cuando se utiliza el comando **`mount -o discard`**. En el sistema operativo Windows, NTFS lleva a cabo anulaciones de asignación en línea de forma predeterminada.

La capacidad de anulación de asignación está deshabilitada de forma predeterminada. Para habilitar la anulación de asignación en un clúster de vSAN, utilice el siguiente comando de RVC: **`vsan.unmap_support –enable`**

Cuando habilite la anulación de asignación en un clúster de vSAN, deberá apagar y volver a encender todas las máquinas virtuales. Las máquinas virtuales deben usar hardware virtual versión 13 o posterior para poder realizar operaciones de anulación de asignación.

Uso de la desduplicación y compresión

vSAN puede realizar la desduplicación y compresión a nivel de bloque para ahorrar espacio de almacenamiento. Cuando habilite la desduplicación y compresión en un clúster basado íntegramente en tecnología flash de vSAN, se reducen los datos redundantes dentro de cada grupo de discos.

La desduplicación elimina los bloques de datos redundantes, mientras que la compresión elimina los datos redundantes adicionales dentro de cada bloque de datos. Estas técnicas funcionan en conjunto para reducir la cantidad de espacio requerido para almacenar los datos. vSAN aplica la desduplicación y luego la compresión a medida que traslada los datos desde el nivel de memoria caché al nivel de capacidad.

Puede habilitar la desduplicación y compresión como una configuración integral del clúster, pero se aplican en cada grupo de discos en particular. Cuando habilite la desduplicación y compresión en un clúster de vSAN, se reducen los datos redundantes dentro de un grupo de discos en particular a una sola copia.

Puede habilitar la desduplicación y compresión cuando cree un clúster basado íntegramente en tecnología flash de vSAN nuevo o cuando edite un clúster basado íntegramente en tecnología flash de vSAN existente. Para obtener más información sobre la creación y la edición de clústeres de vSAN, consulte "Habilitar vSAN" en *Planificar e implementar vSAN*.

Cuando habilite o deshabilite la desduplicación y compresión, vSAN realizará un reformateo secuencial de cada grupo de discos de cada host. De acuerdo con los datos almacenados en el almacén de datos de vSAN, este proceso podría demorar bastante tiempo. No realice estas operaciones con frecuencia. Si planifica deshabilitar la desduplicación y compresión, deberá verificar en primer lugar que exista suficiente capacidad física para colocar los datos.

Nota Puede que la desduplicación y la compresión no sean efectivas para las máquinas virtuales cifradas, ya que el cifrado de las máquinas virtuales cifra los datos del host antes de escribirlos fuera del almacenamiento. Tenga en cuenta los intercambios de almacenamiento cuando use el cifrado de máquinas virtuales.

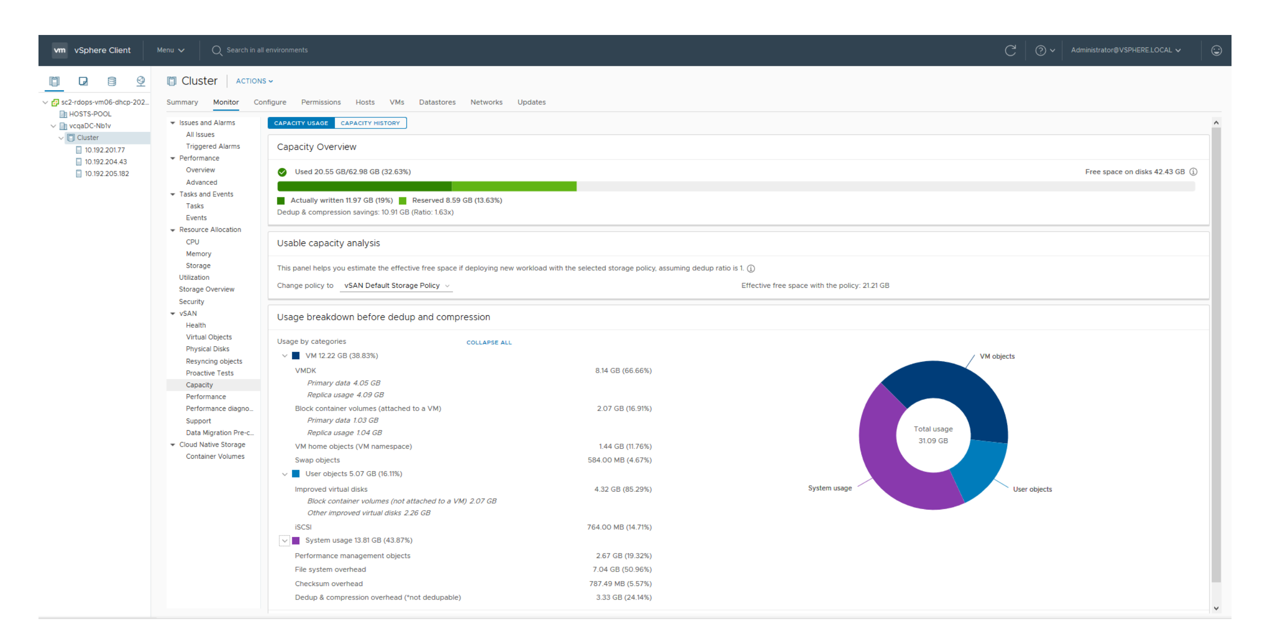
Cómo administrar los discos en un clúster con desduplicación y compresión

Considere las siguientes directrices al administrar discos en un clúster con la desduplicación y compresión habilitadas.

- Evite agregar discos a un grupo de discos de forma incremental. Para lograr una desduplicación y una compresión más eficientes, considere agregar un grupo de discos para aumentar la capacidad de almacenamiento del clúster.
- Cuando incorpore un grupo de discos de forma manual, agregue todos los discos de capacidad al mismo tiempo.
- No es posible eliminar un solo disco de un grupo de discos. Deberá eliminar el grupo de discos entero para realizar modificaciones.
- El error de un solo disco provocará errores en el grupo de discos entero.

Cómo verificar los ahorros de espacio generados por la desduplicación y compresión

La cantidad de reducción de espacio generada por la desduplicación y compresión depende de varios factores, incluido el tipo de datos almacenados y la cantidad de bloques duplicados. Los grupos de discos más grandes tienden a brindar una proporción de desduplicación más elevada. Para comprobar los resultados de la desduplicación y la compresión, puede consultar el desglose del uso antes de la desduplicación y la compresión en el monitor de capacidad de vSAN.



Puede ver el desglose del uso antes de la desduplicación y la compresión cuando supervisa la capacidad de vSAN en vSphere Client. Muestra información sobre los resultados de la desduplicación y compresión. El espacio Usado antes indica el espacio lógico requerido antes de aplicar la desduplicación y compresión, mientras que el espacio Usado después indica el espacio físico usado después de aplicar la desduplicación y compresión. El espacio Usado después también muestra una descripción general de la cantidad de espacio ahorrado, y la proporción de la desduplicación y compresión.

La proporción de desduplicación y compresión se basa en el espacio Usado antes lógico requerido para almacenar los datos antes de la implementación de la desduplicación y compresión, en relación con el espacio Usado después físico requerido después de aplicar la desduplicación y compresión. Específicamente, la proporción es el espacio Usado antes dividido por el espacio Usado después. Por ejemplo, si el espacio Usado antes es 3 GB, pero el espacio Usado después físico es 1 GB, la proporción de desduplicación y compresión es 3x.

Cuando se habilitan la desduplicación y la compresión en el clúster de vSAN, es posible que las actualizaciones de capacidad demoren varios minutos en aparecer en Supervisión de capacidad, a medida que se va reclamando y reasignando el espacio de disco.

Consideraciones de diseño de desduplicación y compresión

Considere estas directrices al configurar la desduplicación y compresión en un clúster de vSAN.

- La desduplicación y compresión están disponibles solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir la desduplicación y compresión.
- Deberá tener una licencia válida para poder habilitar la desduplicación y compresión en un clúster.

- Cuando habilite la desduplicación y compresión en un clúster de vSAN, todos los grupos de discos participarán en la reducción de datos a través de la desduplicación y compresión.
- vSAN puede eliminar los bloques de datos duplicados dentro de cada grupo de discos, pero no entre los grupos de discos.
- La sobrecarga de capacidad para la desduplicación y compresión es aproximadamente un 5 % de la capacidad en bruto total.
- Las directivas deben tener reservas de espacio de objeto del 0 o del 100 %. Las directivas con reservas de espacio de objeto del 100 % siempre se respetan, pero pueden reducir la eficiencia de la desduplicación y la compresión.

Habilitar la desduplicación y la compresión en un nuevo clúster de vSAN

Puede habilitar la desduplicación y la compresión cuando se configura un nuevo clúster basado íntegramente en tecnología flash de vSAN.

Procedimiento

1 Desplácese hasta un nuevo clúster de vSAN basado en flash.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios** y haga clic en **Editar**. b Habilite Desduplicación y compresión. c (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales mientras se habilitan la desduplicación y la compresión. Para obtener más información, consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.
vSphere Web Client	a En vSAN, seleccione **General**. b Haga clic en el botón **Configurar vSAN**. c Configure la desduplicación y la compresión en el clúster. 1 En la página **vSAN capabilites** (Funcionalidades de vSAN), marque la casilla **Enable** (Habilitar) en Deduplication and Compression (Desduplicación y compresión). 2 Habilite la redundancia reducida de las máquinas virtuales. Consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN. d En la página **Reclamar discos**, especifique los discos que se reclamarán para el clúster de vSAN. 1 Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en el icono **Claim for capacity tier** (Recuperar para nivel de capacidad) (). 2 Seleccione un dispositivo flash que se utilizará para almacenamiento en caché y haga clic en el icono **Claim for cache tier** (Recuperar para nivel de almacenamiento en caché) ().

3 Complete la configuración del clúster.

Habilitar la desduplicación y la compresión en un clúster de vSAN existente

Puede habilitar la desduplicación y la compresión mediante la edición de los parámetros de configuración de un clúster de vSAN basado en flash existente.

Requisitos previos

Cree un clúster de vSAN basado en flash.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios**. b Haga clic en **Editar**. c Habilite Desduplicación y compresión. d (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales mientras se habilitan la desduplicación y la compresión. Consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.
vSphere Web Client	a En vSAN, seleccione **General**. b En el panel vSAN is turned ON (vSAN está activado), haga clic en el botón **Edit** (Editar). c Configure la desduplicación y la compresión en el clúster. 1 Establezca la desduplicación y la compresión como **Habilitado**. 2 Habilite la redundancia reducida de las máquinas virtuales. Consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.

3 Haga clic en **Aplicar** o en **Aceptar** para guardar los cambios de configuración.

Resultados

Mientras se habilitan la desduplicación y la compresión, vSAN actualiza el formato en disco de cada grupo de discos del clúster. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

La operación de habilitación no requiere migración de máquinas virtuales ni DRS. El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Deshabilitar la desduplicación y la compresión

Puede deshabilitar la desduplicación y la compresión en el clúster de vSAN.

Cuando se deshabilitan la desduplicación y la compresión en el clúster de vSAN, se puede expandir el tamaño de la capacidad usada en el clúster (en función de la proporción de desduplicación). Antes de deshabilitar la desduplicación y la compresión, compruebe que el clúster tenga suficiente capacidad para gestionar el tamaño de los datos ampliados.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

Opción	Descripción
vSphere Client	a En vSAN, seleccione **Servicios**. b Haga clic en **Editar**. c Deshabilite la desduplicación y la compresión. d (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales a la vez que se deshabilitan la desduplicación y la compresión. Consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.
vSphere Web Client	a En vSAN, seleccione **General**. b En el panel vSAN is turned ON (vSAN está activado), haga clic en el botón **Edit** (Editar). c Deshabilite la desduplicación y la compresión. 1 Establezca el modo de reclamo de discos como **Manual**. 2 Establezca la desduplicación y la compresión como **Deshabilitado**.

3 Haga clic en **Aplicar** o en **Aceptar** para guardar los cambios de configuración.

Resultados

Mientras se deshabilitan la desduplicación y la compresión, vSAN cambia el formato de disco de todos los grupos de discos del clúster. Evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un formato que no admite desduplicación y compresión.

El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Reducir la redundancia de la máquina virtual para el clúster de vSAN

Cuando se habilitan la desduplicación y la compresión, en algunos casos, puede que sea necesario reducir el nivel de protección de las máquinas virtuales.

Habilitar la desduplicación y la compresión requiere un cambio de formato de los grupos de discos. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

En algunos entornos, puede que el clúster de vSAN no tenga suficientes recursos para evacuar por completo el grupo de discos. Un ejemplo de dicha implementación puede ser un clúster de tres nodos sin recursos para evacuar la réplica o el testigo manteniendo una protección completa. Otro ejemplo consiste en un clúster de cuatro nodos con objetos RAID-5 ya implementados. En el último caso, no habrá espacio para mover parte de la fracción RAID-5, ya que los objetos RAID-5 requieren un mínimo de cuatro nodos.

Aún así, se podrán habilitar la desduplicación y la compresión, y usar la opción Permitir redundancia reducida. Esta opción mantiene las máquinas virtuales en ejecución, pero puede que estas no sean capaces de tolerar el nivel total de errores definidos en la directiva de almacenamiento de máquina virtual. Por tanto, durante el cambio de formato para la desduplicación y la compresión, existiría el riesgo temporal de que las máquinas virtuales perdiesen datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la conversión de formato.

Agregar o quitar discos con desduplicación y compresión habilitadas

Cuando se agregan discos a un clúster de vSAN donde se han habilitado la desduplicación y la compresión, se aplican unas consideraciones específicas.

- Puede agregar un disco de capacidad a un grupo de discos con la desduplicación y la compresión habilitadas. No obstante, para una desduplicación y compresión más eficientes, en vez de agregar discos de capacidad, cree un grupo de discos para aumentar la capacidad de almacenamiento del clúster.
- Cuando se quita un discos de un nivel de memoria caché, se quita el grupo de discos completo. Si se quita un disco de nivel de memoria caché cuando la desduplicación y la compresión están habilitadas, se activa la evacuación de datos.
- La desduplicación y la compresión se implementan a nivel de grupo de discos. No puede quitar un disco de capacidad del clúster con la desduplicación y la compresión habilitadas. Deberá eliminar el grupo de discos completo.
- Si se produce un error en un disco de capacidad, no se podrá acceder a ninguno de los discos del grupo. Para solucionar este problema, identifique y sustituya el componente con errores inmediatamente. Al quitar el grupo de discos, use la opción Sin migración de datos.

Usar la codificación de borrado RAID 5 o RAID 6

Puede utilizar la codificación de borrado RAID 5 o RAID 6 para ofrecer una protección frente a la pérdida de datos y aumentar la eficiencia del almacenamiento. La codificación de borrado puede proporcionar el mismo nivel de protección de datos que el reflejo (RAID 1) y, al mismo tiempo, usar menos capacidad de almacenamiento.

La codificación de borrado RAID 5 o RAID 6 permite que vSAN tolere los errores de hasta dos dispositivos de capacidad del almacén de datos. Puede configurar RAID 5 en clústeres basados íntegramente en tecnología flash con cuatro o más dominios de errores. Puede configurar RAID 5 o RAID 6 en clústeres basados íntegramente en tecnología flash con seis o más dominios de errores.

La codificación de borrado RAID 5 o RAID 6 requiere menos capacidad adicional para proteger los datos en comparación con el reflejo RAID 1. Por ejemplo, una máquina virtual protegida con un valor de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) de 1 con RAID 1 requiere el doble del tamaño de disco virtual. Sin embargo, con RAID 5, se requiere 1,33 veces el tamaño de disco virtual. La siguiente tabla muestra una comparación general entre RAID 1 y RAID 5 o RAID 6.

Tabla 6-1. Capacidad requerida para almacenar y proteger los datos con diferentes niveles de RAID

Configuración de RAID	Nivel principal de errores que se toleran	Tamaño de los datos	Capacidad requerida
RAID 1 (reflejo)	1	100 GB	200 GB
RAID 5 o RAID 6 (codificación de borrado) con cuatro dominios de errores	1	100 GB	133 GB
RAID 1 (reflejo)	2	100 GB	300 GB
RAID 5 o RAID 6 (codificación de borrado) con seis dominios de errores	2	100 GB	150 GB

La codificación de borrado RAID 5 o RAID 6 es un atributo de directiva que puede aplicar a los componentes de las máquinas virtuales. Para utilizar RAID 5, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 1. Para utilizar RAID 6, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-5/6 (Erasure Coding) - Capacity** (RAID-5/6 [codificación de borrado]: capacidad) y **Primary level of failures to tolerate** (Nivel principal de errores que se toleran) en 2. La codificación de borrado RAID 5 o RAID 6 no admite un valor de 3 de **Primary level of failures to tolerate** (Nivel principal de errores que se toleran).

Para utilizar RAID 1, establezca **Failure tolerance method** (Método de tolerancia ante errores) en **RAID-1 (Mirroring) - Performance** (RAID-1 [reflejo]: rendimiento). El reflejo RAID 1 requiere menos operaciones de E/S en los dispositivos de almacenamiento y, por lo tanto, puede proporcionar un mejor rendimiento. Por ejemplo, una resincronización del clúster demora menos tiempo en completarse con RAID 1.

Nota En un clúster ampliado de vSAN, el **Método de tolerancia a errores** de **RAID-5/6 (codificación de borrado): capacidad** se aplica únicamente a **Nivel secundario de errores que se toleran**.

Para obtener más información sobre la configuración de las directivas, consulte Capítulo 3 Usar las directivas de vSAN.

Consideraciones de diseño de RAID 5 o RAID 6

Considere estas directrices al configurar la codificación de borrado RAID 5 o RAID 6 en un clúster de vSAN.

- La codificación de borrado RAID 5 o RAID 6 está disponible solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir RAID 5 o RAID 6.
- Deberá tener una licencia válida para poder habilitar RAID 5/6 en un clúster.
- Puede lograr ahorros de espacio adicionales al habilitar la desduplicación y la compresión en el clúster de vSAN.

Usar cifrado en un clúster de vSAN

7

Es posible utilizar el cifrado de datos en reposo para proteger los datos en el clúster de vSAN.

vSAN puede realizar cifrado de datos en reposo. Los datos se cifran después de que se llevan a cabo todas las otras operaciones de procesamiento, como la desduplicación. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.

Para utilizar el cifrado en el clúster de vSAN, se requiere algo de preparación. Una vez que el entorno está configurado, se puede habilitar el cifrado en el clúster de vSAN.

El cifrado de vSAN requiere un servidor de administración de claves (Key Management Server, KMS) externo, el sistema vCenter Server y los hosts ESXi. vCenter Server solicita claves de cifrado desde un KMS externo. El KMS genera y almacena las claves, y vCenter Server obtiene los identificadores de claves del KMS y los distribuye en los hosts ESXi.

vCenter Server no almacena las claves del KMS, pero sí conserva una lista de identificadores de claves.

Este capítulo incluye los siguientes temas:

Cómo funciona el cifrado de vSAN

Cuando se habilita el cifrado, vSAN cifra todo el contenido del almacén de datos de vSAN. Como se cifra la totalidad de los archivos, todas las máquinas virtuales y sus correspondientes datos quedan protegidos. Solo los administradores con privilegios de cifrado puede realizar tareas de cifrado y descifrado.

vSAN utiliza las claves de cifrado de la siguiente manera:

- vCenter Server solicita a KMS una clave de cifrado de claves (Key Encryption Key, KEK) AES-256. vCenter Server almacena solo el identificador de la KEK, pero no la clave en sí.
- El host ESXi cifra los datos del disco mediante el modo AES-256 XTS estándar del sector. Cada disco tiene una clave de cifrado de datos (Data Encryption Key, DEK) diferente que se genera al azar.
- Cada host ESXi usa la KEK para cifrar sus DEK y almacena las DEK cifradas en el disco. El host no almacena la KEK en el disco. Si un host se reinicia, solicita a KMS la KEK con el identificador correspondiente. A continuación, el host puede descifrar sus DEK según lo necesite.
- La clave de un host no se usa para cifrar datos, sino volcados de núcleos. Todos los hosts de un mismo clúster usan la misma clave de host. Al recopilar paquetes de soporte, se genera una clave al azar para volver a cifrar los volcados de núcleo. Puede especificar una contraseña para cifrar la clave aleatoriamente.

Cuando un host se reinicia, no monta sus grupos de discos hasta recibir la KEK. Este proceso puede tardar varios minutos o más en completarse. Es posible supervisar el estado de los grupos de discos en vSAN Health Service, en **Discos físicos > Estado de software**.

Consideraciones de diseño para el cifrado de vSAN

Tenga en cuenta las siguientes directrices al trabajar con el cifrado de vSAN.

- No implemente el servidor KMS en el mismo almacén de datos de vSAN que planea cifrar.
- El cifrado requiere gran consumo de CPU. AES-NI mejora significativamente el rendimiento del cifrado. Habilite AES-NI en el BIOS.
- El host testigo de un clúster ampliado no participa en el cifrado de vSAN. Solo se almacenan metadatos en el host testigo.
- Establezca una directiva con respecto a los volcados de núcleo. Los volcados de núcleo están cifrados porque pueden contener información confidencial, por ejemplo, claves. Al descifrar un volcado de núcleo, maneje la información confidencial con cuidado. Los volcados de núcleo de ESXi pueden contener claves para el host ESXi y para los datos que este contiene.
  - Siempre utilice una contraseña cuando recopile un paquete de `vm-support`. Puede especificar la contraseña cuando genera el paquete de soporte de vSphere Client o puede utilizar el comando `vm-support`.

    La contraseña vuelve a cifrar los volcados de núcleo que utilizan claves internas de manera que estos volcados empleen claves basadas en la contraseña. Posteriormente, se puede usar la contraseña para descifrar cualquier volcado de núcleo cifrado que pudiera estar incluido en el paquete de soporte. Esto no afecta a los volcados de núcleo ni a los registros que estén sin cifrar.

- La contraseña que especificó durante la creación del paquete de `vm-support` no persiste en los componentes de vSphere. Es su responsabilidad llevar un registro de las contraseñas de los paquetes de soporte.

Configurar el clúster de KMS

Un clúster de servidor de administración de claves (Key Management Server, KMS) proporciona las claves que pueden usarse para cifrar el almacén de datos de vSAN.

Para poder cifrar el almacén de datos de vSAN, se debe configurar un clúster de KMS a fin de admitir el cifrado. Esa tarea incluye agregar el KMS a vCenter Server y establecer confianza con el KMS. vCenter Server proporciona claves de cifrado desde el clúster de KMS.

KMS debe admitir el estándar del protocolo de interoperabilidad para la administración de claves (Key Management Interoperability Protocol, KMIP) 1.1.

Agregar un KMS a vCenter Server

Los servidores de administración de claves (KMS) se agregan a los sistemas vCenter Server desde vSphere Client.

vCenter Server crea un clúster de KMS cuando agrega la primera instancia de KMS. Si configura el clúster de KMS en dos o más instancias de vCenter Server, asegúrese de usar el mismo nombre de clúster de KMS.

Nota No implemente los servidores KMS en el clúster de vSAN que planea cifrar. Si se produce un error, los hosts del clúster de vSAN deberán comunicarse con el servidor KMS.

- Cuando agrega el KMS, se le solicita establecer este clúster como predeterminado. Más adelante, puede cambiar explícitamente el clúster predeterminado.
- Una vez que vCenter Server crea el primer clúster, puede agregar instancias de KMS del mismo proveedor al clúster y configurar todas las instancias de KMS para sincronizar las claves entre ellos. Utilice el método documentado por el proveedor de KMS.
- Puede configurar el clúster con una sola instancia de KMS.
- Si el entorno admite soluciones de KMS de diferentes proveedores, puede agregar varios clústeres de KMS.

Requisitos previos

- Compruebe que el servidor de claves se encuentre en *Matrices de compatibilidad de vSphere* y que cumpla con KMIP 1.1.
- Compruebe que dispone de los privilegios necesarios: **Cryptographer.ManageKeyServers (Criptógrafo.AdministrarServidoresClaves).**
- No se admite la conexión con un KMS exclusivamente por medio de una dirección IPv6.

- No se admite la conexión con un KMS a través de un servidor proxy que requiera nombre de usuario o contraseña.

Procedimiento

1 Inicie sesión en vCenter Server.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y en **Servidores de administración de claves**.

4 Haga clic en **Agregar**, especifique la información de KMS en el asistente y haga clic en **Aceptar**.

Opción	Valor
clúster de KMS	Seleccione **Crear nuevo clúster** para crear un nuevo clúster. Si existe un clúster, puede seleccionarlo.
Nombre del clúster	Nombre del clúster de KMS. Puede utilizar este nombre para conectarse al KMS si la instancia de vCenter Server deja de estar disponible.
Alias de servidor	Alias del KMS. Puede utilizar este alias para conectarse al KMS si la instancia de vCenter Server deja de estar disponible.
Dirección de servidor	Dirección IP o FQDN del KMS.
Puerto de servidor	Puerto en el cual vCenter Server se conecta al KMS.
Dirección de proxy	Dirección de proxy opcional para conectarse al KMS.
Puerto de proxy	Puerto de proxy opcional para conectarse al KMS.
Nombre de usuario	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar claves de cifrado utilizadas por distintos usuarios o grupos. Especifique un nombre de usuario solo si el KMS admite esta funcionalidad y si piensa utilizarla.
Contraseña	Algunos proveedores de KMS permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar claves de cifrado utilizadas por distintos usuarios o grupos. Especifique una contraseña solo si el KMS admite esta funcionalidad y si piensa utilizarla.

Establecer una conexión de confianza mediante el intercambio de certificados

Después de agregar el KMS al sistema de vCenter Server, puede establecer una conexión de confianza. El proceso exacto depende de los certificados que el KMS acepte y de la directiva de la empresa.

Requisitos previos

Agregue el clúster KMS.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Haga clic en **Establecer confianza con KMS**.

5 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz	Usar la opción Certificado de CA raíz para establecer una conexión de confianza.
Certificado	Usar la opción Certificado para establecer una conexión de confianza.
Nueva solicitud de firma de certificado	Usar la opción New Certificate Signing Request (Nueva solicitud de firma del certificado) para establecer una conexión de confianza.
Cargar certificado y clave privada	Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza.

Usar la opción Certificado de CA raíz para establecer una conexión de confianza

Algunos proveedores de KMS, como SafeNet, requieren que se cargue un certificado de CA raíz al KMS. Este KMS establece una conexión de confianza con todos los certificados firmados por la entidad de certificación de raíz.

El certificado de CA raíz que utiliza el cifrado de máquinas virtuales de vSphere es un certificado autofirmado que se almacena en un almacén separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Nota Genere un certificado de CA raíz solo si desea reemplazar los certificados existentes. En ese caso, los demás certificados que están firmados por esa entidad de certificación raíz dejan de ser válidos. Se puede generar un nuevo certificado de CA raíz como parte de este flujo de trabajo.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificado de CA raíz** y haga clic en **Aceptar**.

   El cuadro de diálogo Descargar certificado de CA raíz se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al sistema.

   Nota Algunos proveedores de KMS, por ejemplo SafeNet, requieren que el proveedor de KMS reinicie el KMS para seleccionar el certificado raíz que se cargó.

Pasos siguientes

Finalice el intercambio de certificados. Consulte Completar la instalación de confianza.

Usar la opción Certificado para establecer una conexión de confianza

Algunos proveedores de KMS, como Vormetric, requieren que se cargue el certificado de vCenter Server al KMS. Después de la carga, el KMS acepta el tráfico proveniente de un sistema con ese certificado.

vCenter Server genera un certificado para proteger las conexiones con el KMS. El certificado se almacena en un almacén de claves separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Certificado** y haga clic en **Aceptar**.

   El cuadro de diálogo Descargar certificado se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

   Nota No genere un certificado nuevo a menos que desee reemplazar los certificados existentes.

5 Copie el certificado en el portapapeles o descárguelo como un archivo.

6 Siga las instrucciones de su proveedor de KMS para cargar el certificado al KMS.

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Usar la opción New Certificate Signing Request (Nueva solicitud de firma del certificado) para establecer una conexión de confianza

Algunos proveedores de KMS, por ejemplo Thales, requieren que vCenter Server genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y que se envíe esa CSR al KMS. El KMS firma la CSR y devuelve el certificado firmado. El certificado firmado se puede cargar en vCenter Server.

El uso de la opción **New Certificate Signing Request** (Nueva solicitud de firma del certificado) es un proceso de dos pasos. Primero debe generar la CSR y enviarla al proveedor de KMS. A continuación, cargue el certificado firmado que recibió del proveedor de KMS a vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **New Certificate Signing Request** (Nueva solicitud de firma del certificado) y haga clic en **OK** (Aceptar).

5 En el cuadro de diálogo, copie el certificado completo del cuadro de texto en el portapapeles o descárguelo como un archivo, y haga clic en **OK** (Aceptar).

   Use el botón **Generate new CSR** (Generar nueva CSR) del cuadro de diálogo únicamente si desea generar una CSR de forma explícita. Al usar esa opción, todos los certificados firmados basados en la CSR anterior dejan de ser válidos.

6 Siga las instrucciones de su proveedor de KMS para enviar la CSR.

7 Cuando reciba el certificado firmado del proveedor de KMS, vuelva a hacer clic en **Key Management Servers** (Servidores de administración de claves) y vuelva a seleccionar **New Certificate Signing Request** (Nueva solicitud de firma del certificado).

8 Pegue el certificado firmado en el cuadro de texto inferior o haga clic en **Upload File** (Cargar archivo) y cargue el archivo; luego, haga clic en **OK** (Aceptar).

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza

Algunos proveedores de KMS, como HyTrust, requieren que se cargue el certificado del servidor KMS y la clave privada al sistema de vCenter Server.

Algunos proveedores de KMS generan un certificado y una clave privada para la conexión y los vuelven disponibles para el usuario. Una vez que haya cargado los archivos, el KMS establecerá una conexión de confianza con su instancia de vCenter Server.

Requisitos previos

- Solicite un certificado y una clave privada al proveedor de KMS. Los archivos son archivos X509 en formato PEM.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Seleccione **Cargar certificado y clave privada** y haga clic en **Aceptar**.

5 Pegue el certificado que recibió del proveedor de KMS en el cuadro de texto superior o haga clic en **Cargar certificado** para cargar el archivo del certificado.

6 Pegue el archivo de claves en el cuadro de texto inferior o haga clic en **Cargar archivo** para cargar el archivo de claves.

7 Haga clic en **Aceptar**.

Pasos siguientes

Finalice la relación de confianza. Consulte Completar la instalación de confianza.

Establecer el clúster de KMS como predeterminado

Si no establece el primer clúster como el clúster predeterminado o si el entorno usa varios clústeres y elimina el clúster predeterminado, debe establecer el clúster de KMS como predeterminado.

Requisitos previos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña **Servidores de administración de claves** sea Normal y con una marca de verificación verde.

Procedimiento

1 Desplácese hasta el sistema vCenter Server.

2 Haga clic en la pestaña **Configurar** y en **Servidores de administración de claves** en **Más**.

3 Seleccione el clúster y haga clic en **Establecer el clúster de KMS como predeterminado**.

   No seleccione el servidor. El menú para establecer el clúster como predeterminado está disponible para ese clúster solamente.

4 Haga clic en **Sí**.

   La palabra `default` aparece junto al nombre del clúster.

Completar la instalación de confianza

A menos que el cuadro de diálogo **Agregar servidor** le haya solicitado confiar en el KMS, debe establecer la confianza explícitamente una vez finalizado el intercambio de certificados.

Es posible completar la instalación de confianza, es decir, hacer que vCenter Server confíe en el KMS, ya sea confiando en el KMS o cargando un certificado de KMS. Tiene dos opciones:

- Confiar en el certificado explícitamente por medio de la opción **Actualizar certificado de KMS**.
- Cargar un certificado de hoja de KMS o el certificado de CA de KMS en vCenter Server por medio de la opción **Cargar certificado de KMS**.

Nota Si carga el certificado de CA raíz o el certificado de CA intermedia, vCenter Server confía en todos los certificados que firma esa CA. Si desea obtener una seguridad más solida, cargue un certificado de hoja o un certificado de CA intermedia que controle el proveedor de KMS.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Servidores de administración de claves**.

3 Seleccione la instancia de KMS con la cual desea establecer una conexión de confianza.

4 Para establecer la relación de confianza, actualice o cargue el certificado de KMS.

Opción	Acción
Actualizar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Actualizar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Confiar**.
Cargar certificado de KMS	a Haga clic en **Todas las acciones** y seleccione **Cargar certificado de KMS**. b En el cuadro de diálogo que aparece, haga clic en **Cargar archivo**, cargue un archivo de certificado y haga clic en **Aceptar**.

Habilitar el cifrado en un nuevo clúster de vSAN

Puede habilitar el cifrado cuando se configura un nuevo clúster de vSAN.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.

Procedimiento

1 Desplácese hasta un clúster existente.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios** y haga clic en el botón **Editar cifrado**.

4 En el cuadro de diálogo **Servicios de vSAN**, habilite el **Cifrado** y seleccione un clúster de KMS.

Nota Asegúrese de que no esté marcada la casilla **Erase disks before use** (Borrar discos antes del uso), a menos que desee borrar los datos actuales de los dispositivos de almacenamiento durante el cifrado.

5 Complete la configuración del clúster.

Resultados

En el clúster de vSAN, se habilita el cifrado de datos en reposo. vSAN cifra todos los datos que se agregan al almacén de datos de vSAN.

Generar nuevas claves de cifrado

Es posible crear nuevas claves de cifrado en caso de que una clave caduque o se vea comprometida.

Al generar nuevas claves de cifrado para el clúster de vSAN, están disponibles las siguientes opciones:

- Si genera una nueva KEK, todos los hosts del clúster de vSAN reciben la nueva KEK del KMS. La DEK de cada host se vuelve a cifrar con la nueva KEK.
- Si elige volver a cifrar todos los datos con claves nuevas, se generan una nueva KEK y una nueva DEK. Para volver a cifrar los datos, es preciso reformatear el disco en forma sucesiva.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.

Procedimiento

1. Desplácese hasta el clúster del host de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Servicios**.
4. Haga clic en **Generar nuevas claves de cifrado**.
5. Para generar una nueva KEK, haga clic en **Aplicar**. Las DEK se volverán a cifrar con la nueva KEK.
   - Para generar una nueva KEK y nuevas DEK, y para volver a cifrar todos los datos del clúster de vSAN, active la siguiente casilla: **También vuelva a cifrar todos los datos en el almacenamiento con nuevas claves**.
   - Si el clúster de vSAN tiene recursos limitados, marque la casilla **Permitir redundancia reducida**. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

Habilitar el cifrado de vSAN en un clúster de vSAN existente

Puede habilitar el cifrado mediante la edición de los parámetros de configuración de un clúster de vSAN existente.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Se debe haber configurado un clúster de KMS y establecido una conexión de confianza entre vCenter Server y KMS.
- El reclamo de discos del clúster debe estar configurado en modo manual.

Procedimiento

1. Desplácese hasta el clúster del host de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Servicios**.
4. Haga clic en el botón **Editar cifrado**.
5. En el cuadro de diálogo Servicios de vSAN, habilite el **Cifrado** y seleccione un clúster de KMS.
6. (Opcional) Si los dispositivos de almacenamiento del clúster contienen datos confidenciales, selecciona **Borrar discos antes del uso**.

   Con esta configuración, vSAN limpia los datos existentes de los dispositivos de almacenamiento durante el cifrado. Esta opción puede aumentar el tiempo para procesar cada disco, así que no la seleccione a menos que tenga datos no deseados en los discos.
7. Haga clic en **Aplicar**.

Resultados

Se lleva a cabo un reformateo sucesivo de todos los grupos de discos mientras vSAN cifra todos los datos en el almacén de datos de vSAN.

Cifrado y volcados de núcleo en vSAN

Si el clúster de vSAN utiliza cifrado y si se produce un error en el host ESXi, el volcado de núcleo resultante se cifra para proteger los datos del cliente. Los volcados de núcleo que se incluyen en el paquete de `vm-support` también están cifrados.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad de datos y privacidad de la organización al gestionar el volcado de núcleo.

Volcados de núcleo en hosts ESXi

Cuando un host ESXi se bloquea, se genera un volcado de núcleo cifrado y el host se reinicia. El volcado de núcleo se cifra con la clave de host que se encuentra en la memoria caché de claves de ESXi. Lo que puede hacer a continuación depende de diversos factores.

- En la mayoría de los casos, vCenter Server recupera la clave del host del KMS e intenta insertar la clave en el host ESXi después de reiniciar. Si la operación se realiza correctamente, se puede generar el paquete de `vm-support` y descifrar o volver a cifrar el volcado de núcleo.
- Si vCenter Server no puede conectarse al host ESXi, tal vez se pueda recuperar la clave del KMS.
- Si el host usó una clave personalizada que no es igual a la clave que vCenter Server inserta en el host, no se podrá manipular el volcado de núcleo. Evite usar claves personalizadas.

Volcados de núcleo y paquetes de vm-support

Si se comunica con el soporte técnico de VMware debido a un error grave, el representante de soporte, por lo general, le pedirá que genere un paquete de `vm-support`. El paquete incluye archivos de registro y otra información, incluso volcados de núcleo. Si los representantes de soporte no pueden resolver los inconvenientes al analizar los archivos de registro y otra información, el usuario puede descifrar los volcados de núcleo para habilitar la información relevante. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Volcados de núcleo de sistemas vCenter Server

Un volcado de núcleo de un sistema vCenter Server no está cifrado. vCenter Server ya contiene información posiblemente confidencial. Como mínimo, asegúrese de que el sistema Windows donde se ejecuta vCenter Server Appliance o que vCenter Server estén protegidos. Asimismo, también se recomienda apagar los volcados de núcleo del sistema de vCenter Server. Otra información de los archivos de registro puede ayudar a determinar el problema.

Recopilar un paquete de vm-support para un host de ESXi en un clúster de vSAN cifrado

Cuando se habilita el cifrado en un clúster de vSAN, se cifran todos los volcados de núcleo en el paquete de `vm-support`. Puede recopilar el paquete y especificar una contraseña si piensa descifrar el volcado de núcleo más adelante.

El paquete de `vm-support` incluye archivos de registro, archivos de volcado de núcleo, entre otros.

Requisitos previos

Notifique a su representante de soporte que se habilitó el cifrado para el clúster de vSAN. Es posible que el representante le pida descifrar los volcados de núcleo para extraer información relevante.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger información confidencial, como claves de host.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Web Client basado en Flex.
2. Haga clic en **Hosts y clústeres** y, a continuación, haga clic con el botón derecho en el host ESXi.
3. Seleccione **Exportar registros del sistema**.
4. En el cuadro de diálogo, seleccione **Contraseña para volcados de núcleo cifrados** y, a continuación, especifique y confirme una contraseña.
5. Deje los valores predeterminados para otras opciones o haga cambios si así lo requiere el soporte técnico de VMware, y haga clic en **Finalizar**.
6. Especifique una ubicación para el archivo.
7. Si su representante de soporte le pidió descifrar el volcado de núcleo en el paquete de `vm-support`, inicie sesión en cualquier host ESXi y siga estos pasos.
   a. Inicie sesión en ESXi y conéctese al directorio donde está ubicado el paquete de `vm-support`.

      El nombre de archivo sigue el patrón **`esx.fecha_y_hora.tgz`**.
   b. Asegúrese de que el directorio tenga suficiente espacio para el paquete, el paquete descomprimido y el paquete nuevamente comprimido; o bien mueva el paquete.
   c. Extraiga el paquete en el directorio local.

      ```
      vm-support -x *.tgz .
      ```

      La jerarquía de archivos resultante puede contener los archivos de volcado de núcleo del host ESXi, generalmente en `/var/core`, y puede contener varios archivos de volcado de núcleo de las máquinas virtuales.

d Descifre cada archivo de volcado de núcleo cifrado por separado.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdumpdecryptedZdump
```

vm-support-incident-key-file es el archivo de clave del incidente que se encuentra en el nivel superior del directorio.

encryptedZdump es el nombre del archivo de volcado de núcleo cifrado.

decryptedZdump es el nombre del archivo que genera el comando. Procure que el nombre sea similar al nombre de *encryptedZdump*.

e Proporcione la contraseña que especificó al crear el paquete de `vm-support`.

f Elimine los volcados de núcleo cifrados y vuelva a comprimir el paquete.

```
vm-support --reconstruct
```

8 Elimine los archivos que contienen información confidencial.

Descifrar o volver a cifrar un volcado de núcleo cifrado

Para descifrar o volver a cifrar un volcado de núcleo cifrado en el host ESXi, puede usar la CLI `crypto-util`.

Puede descifrar y examinar por su cuenta los volcados de núcleo en el paquete de `vm-support`. Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Para obtener detalles sobre cómo volver a cifrar un volcado de núcleo y sobre otras funciones de `crypto-util`, consulte la ayuda de la línea de comandos.

Nota `crypto-util` es para usuarios avanzados.

Requisitos previos

La clave de host ESXi que se usó para cifrar el volcado de núcleo debe estar disponible en el host ESXi que generó el volcado de núcleo.

Procedimiento

1 Inicie sesión directamente en el host ESXi donde se produjo el volcado de núcleo.

Si el host ESXi se encuentra en el modo de bloqueo, o si el acceso SSH está deshabilitado, es posible que deba habilitar el acceso en primer lugar.

2 Determine si el volcado de núcleo está cifrado.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope describe vmmcores.ve`
archivo zdump	`crypto-util envelope describe --offset 4096` *`zdumpFile`*

3 Descifre el volcado de núcleo según su tipo.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope extract vmmcores.ve vmmcores`
archivo zdump	`crypto-util envelope extract --offset 4096` *`zdumpEncryptedzdumpUnencrypted`*

Actualizar el clúster de vSAN

8

La actualización de vSAN es un proceso de varias etapas, en el cual los procedimientos de actualización se deben llevar a cabo en el orden que se describe aquí.

Antes de intentar realizar la actualización, asegúrese de comprender claramente todo el proceso de actualización, a fin de garantizar una actualización correcta y sin interrupciones. Si no está familiarizado con el procedimiento general de actualización de vSphere, primero debe consultar el documento *Actualización de vSphere*.

Nota Si no se respeta la secuencia de tareas para la actualización que se describe aquí, se perderán datos y se producirán errores en el clúster.

La actualización del clúster de vSAN se lleva a cabo en la siguiente secuencia de tareas.

1 Actualización de vCenter Server. Consulte la documentación sobre la *actualización de vSphere*.

2 Actualización de los hosts ESXi hosts. Consulte Actualizar los hosts ESXi. Para obtener información sobre la migración y la preparación para la actualización de los hosts ESXi, consulte el documento *Actualización de vSphere*.

3 Actualice el formato de disco de vSAN. La actualización del formato de disco es opcional, pero, para obtener los mejores resultados, actualice los objetos a la versión más reciente. El formato en disco expone el entorno al conjunto completo de características de vSAN. Consulte Actualizar el formato de disco de vSAN mediante RVC.

Este capítulo incluye los siguientes temas:

Antes de actualizar vSAN

Planifique y diseñe la actualización para que sea a prueba de errores. Antes de intentar actualizar vSAN, compruebe que el entorno cumpla con los requisitos de hardware y software de vSphere.

Requisito previo de actualización

Tenga en cuenta los aspectos que pueden retrasar el proceso general de actualización.
Para obtener instrucciones y prácticas recomendadas, consulte el documento *Actualización de vSphere*.

Revise los requisitos clave antes de actualizar el clúster a vSAN 6.7.3.

Tabla 8-1. Requisito previo de actualización

Requisitos previos de actualización	Descripción
Software, hardware, controladores, firmware y controladoras de E/S de almacenamiento	Compruebe que vSAN 6.7.3 sea compatible con los componentes de software y hardware, los controladores, el firmware y las controladoras de E/S de almacenamiento que planea usar. Los elementos compatibles se enumeran en el sitio web de la guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php.
Versión de vSAN	Compruebe que esté usando la versión más reciente de vSAN. No puede realizar la actualización desde una versión beta a vSAN 6.7.3. Cuando actualice desde una versión beta, debe realizar una implementación nueva de vSAN.
Espacio en disco	Compruebe que tenga espacio suficiente disponible para completar la actualización de la versión de software. La cantidad de almacenamiento en disco que se necesita para la instalación de vCenter Server depende de la configuración de vCenter Server. Para obtener instrucciones sobre el espacio en disco que se necesita para la actualización de vSphere, consulte el documento *Actualización de vSphere* .
Formato de disco de vSAN	Asegúrese de contar con capacidad de almacenamiento suficiente para actualizar el formato de disco. Si no hay espacio disponible igual a la capacidad consumida del grupo de discos más grande, y con espacio disponible en grupos de discos que no son los grupos de discos que se están convirtiendo, debe seleccionar **Permitir redundancia reducida** como la opción de migración de datos. Por ejemplo, el grupo de discos más grande de un clúster tiene 10 TB de capacidad física, pero solamente se están usando 5 TB. Se necesita una capacidad de reserva adicional de 5 TB en otra ubicación del clúster, excepto los grupos de discos que se están migrando. Al actualizar el formato de disco de vSAN, compruebe que los hosts no estén en modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN ingresa en modo de mantenimiento, la capacidad del clúster se reduce de manera automática. El host miembro deja de aportar almacenamiento al clúster y su capacidad deja de estar disponible para los datos. Para obtener información sobre los diversos modos de evacuación, consulte Poner un miembro de un clúster de vSAN en modo de mantenimiento.

Tabla 8-1. Requisito previo de actualización (continuación)

Requisitos previos de actualización	Descripción
Hosts de vSAN	Asegúrese de haber puesto los hosts de vSAN en modo de mantenimiento y de haber seleccionado la opción **Garantizar accesibilidad a los datos** o **Evacuar todos los datos**. Puede usar vSphere Update Manager para automatizar y probar el proceso de actualización. Sin embargo, cuando se usa vSphere Update Manager para actualizar vSAN, el modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Cuando se usa el modo **Garantizar accesibilidad a los datos**, los datos no quedan protegidos y, si ocurre un error durante la actualización de vSAN, es posible que se produzca una pérdida de datos inesperada. No obstante, el modo **Ensure data accessibility** (Garantizar accesibilidad a los datos) es más rápido que el modo **Evacuate all data** (Evacuar todos los datos), ya que no es necesario transferir todos los datos a otro host del clúster. Para obtener información sobre los diversos modos de evacuación, consulte Poner un miembro de un clúster de vSAN en modo de mantenimiento.
Virtual Machines (Máquinas virtuales)	Compruebe que se haya creado una copia de seguridad de las máquinas virtuales.

Recomendaciones

Tenga en cuenta las siguientes recomendaciones al implementar hosts ESXi para su uso con vSAN:

- Si los hosts de ESXi están configurados con una capacidad de memoria de 512 GB o menos, use dispositivos SATADOM, SD, USB o discos duros como medios de instalación.
- Si los hosts de ESXi están configurados con una capacidad de memoria superior a 512 GB, use un dispositivo flash o un disco magnético independiente como dispositivo de instalación. Si usa un dispositivo independiente, compruebe que vSAN no reclama el dispositivo.
- Al arrancar un host vSAN desde un dispositivo SATADOM, debe usar un dispositivo de celdas de un solo nivel (single-level cell, SLC) y el tamaño del dispositivo de arranque debe ser de 16 GB como mínimo.
- Para asegurarse de que el hardware cumpla con los requisitos de vSAN, consulte "Requisitos de hardware de vSAN" en *Planificar e implementar vSAN*.

vSAN 6.5 y las versiones posteriores permiten ajustar los requisitos de tamaño de arranque para un host ESXi en un clúster de vSAN. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2147881.

Actualizar el host testigo en un clúster ampliado o de dos hosts

El host testigo de un clúster de dos hosts o un clúster ampliado se encuentra fuera del clúster de vSAN, pero se administra con la misma instancia de vCenter Server. Es posible usar el mismo proceso para actualizar el host testigo que se usa para un host de datos de vSAN.

No actualice el host testigo hasta que todos los hosts de datos se hayan actualizado y hayan salido del modo de mantenimiento.

El uso de vSphere Update Manager para actualizar hosts en paralelo puede provocar que el host testigo se actualice en paralelo con uno de los hosts de datos. Para evitar problemas de actualización, configure vSphere Update Manager de modo que no actualice el host testigo en paralelo con los hosts de datos.

Actualizar vCenter Server

La primera tarea que se realizará durante la actualización de vSAN es una actualización general de vSphere, que incluye la actualización de vCenter Server y los hosts ESXi.

VMware admite actualizaciones locales en sistemas de 64 bits de vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x y vCenter Server 5.5 a vCenter Server 6.0 y posteriores. La actualización de vCenter Server incluye una actualización del esquema de la base de datos y una actualización de vCenter Server. En lugar de realizar una actualización local a vCenter Server, se puede utilizar otro equipo para llevar a cabo la actualización. Para obtener instrucciones detalladas y varias opciones de actualización, consulte el documento *Actualización de vSphere*.

Actualizar los hosts ESXi

Después de actualizar vCenter Server, la siguiente tarea en la actualización del clúster de vSAN es actualizar los hosts ESXi para que usen la versión actual.

Si tiene varios hosts en el clúster de vSAN y usa vSphere Update Manager para actualizarlos, el modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Si se utiliza este modo y se produce un error durante la actualización de vSAN, es posible que no se pueda acceder a los datos hasta que uno de los hosts vuelva a estar conectado. Para obtener información sobre cómo trabajar con los modos de evacuación, consulte Poner un miembro de un clúster de vSAN en modo de mantenimiento

Antes de intentar realizar una actualización de los hosts ESXi, consulte las prácticas recomendadas que se describen en el documento *Actualización de vSphere*. VMware proporciona varias opciones de actualización de ESXi. Seleccione la opción de actualización que resulte más adecuada para el tipo de host que va a actualizar. Para obtener más información sobre las diversas opciones de actualización, consulte el documento *Actualización de vSphere*.

Requisitos previos

- Compruebe que tenga espacio suficiente en disco para actualizar los hosts ESXi. Para obtener instrucciones en relación con los requisitos de espacio en disco, consulte el documento *Actualización de vSphere*.
- Compruebe que esté usando la versión más reciente de ESXi. Puede descargar el instalador de ESXi más reciente desde el sitio web de descargas de productos VMware: https://my.vmware.com/web/vmware/downloads.

- Compruebe que esté usando la versión más reciente de vCenter Server.
- Compruebe la compatibilidad de la configuración de red, la controladora de E/S de almacenamiento, el dispositivo de almacenamiento y el software de copia de seguridad.
- Compruebe que se haya creado una copia de seguridad de las máquinas virtuales.
- Use Distributed Resource Scheduler (DRS) para prevenir el tiempo de inactividad de las máquinas virtuales durante la actualización. Compruebe que el nivel de automatización de cada máquina virtual se configure en el modo **Fully Automated** (Completamente automatizado) para ayudar a DRS a migrar máquinas virtuales cuando los hosts entran en modo de mantenimiento. Como alternativa, también puede apagar todas las máquinas virtuales o ejecutar una migración manual.

Procedimiento

1 Coloque en modo de mantenimiento el host que desea actualizar.

   Debe comenzar la ruta de acceso de actualización con los hosts ESXi 5.5 o los más recientes en el clúster de vSAN.

   a Haga clic con el botón derecho en el host y seleccione **Maintenance Mode > Enter Maintenance Mode** (Modo de mantenimiento > Entrar en modo de mantenimiento).

   b Seleccione el modo de evacuación **Ensure data accessibility** (Garantizar accesibilidad a los datos) o **Evacuate all data** (Evacuar todos los datos), según sus requisitos, y espere hasta que el host entre en modo de mantenimiento.

      Si usa vSphere Update Manager para actualizar el host, o si trabaja con un clúster de tres hosts, el modo de evacuación predeterminado disponible es **Ensure data accessibility** (Garantizar accesibilidad a los datos). Este modo es más rápido que el modo **Evacuate all data** (Evacuar todos los datos). Sin embargo, el modo **Ensure data accessibility** (Garantizar accesibilidad a los datos) no ofrece protección completa para los datos. Si se produce un error en el host durante las operaciones del modo de mantenimiento, es posible que no se pueda acceder a algunos datos hasta que uno de los hosts vuelva a estar conectado.

2 Cargue el software en el almacén de datos del host ESXi y compruebe que el archivo esté disponible en el directorio dentro del almacén de datos. Por ejemplo, puede cargar el software en `/vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip`.

3 Ejecute el comando `esxcliinstall -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check`. Use el VIB de software `esxcli` para ejecutar este comando.

   Una vez que el host ESXi se haya instalado correctamente, verá el siguiente mensaje:

   `The update completed successfully, but the system needs to be rebooted for the changes to be effective.` (La actualización ha finalizado correctamente, pero es necesario reiniciar el sistema para que se apliquen los cambios).

4 Reinicie manualmente el host de ESXi.

   a Desplácese hasta el host de ESXi en el inventario.

   b Haga clic con el botón derecho en el host, seleccione **Encender > Reiniciar**, haga clic en **Sí** para confirmar y espere hasta que se reinicie el host.

   c Haga clic con el botón derecho en el host, seleccione **Connection > Disconnect** (Conexión > Desconectar) y, a continuación, seleccione **Connection > Connect** (Conexión > Conectar) para volver a conectarse al host.

   Para actualizar los hosts restantes del clúster, repita este procedimiento para cada host.

   Si tiene varios hosts en el clúster de vSAN, puede usar vSphere Update Manager para actualizar los hosts restantes.

5 Salga del modo de mantenimiento.

Pasos siguientes

1 (opcional) Actualice el formato de disco de vSAN. Consulte Actualizar el formato de disco de vSAN mediante RVC.

2 Compruebe la licencia del host. En la mayoría de los casos, deberá volver a aplicar la licencia del host. Para obtener información acerca de cómo aplicar licencias de hosts, consulte el documento sobre la *administración de vCenter Server y hosts*.

3 (opcional) Actualice las máquinas virtuales en los hosts mediante vSphere Client o vSphere Update Manager.

Acerca del formato de disco de vSAN

La actualización del formato de disco es opcional. El clúster de vSAN seguirá funcionando correctamente si utiliza una versión de formato de disco anterior.

Para obtener mejores resultados, actualice los objetos para que usen la versión de formato en disco más reciente. El formato en disco más reciente proporciona el conjunto completo de características de vSAN.

Según el tamaño de los grupos de discos, la actualización del formato de disco puede ser lenta, debido a que los grupos de discos se actualizan de a uno por vez. Para cada actualización de grupo de discos, se evacúan todos los datos de cada dispositivo y se quita el grupo de discos del clúster de vSAN. Luego, el grupo de discos vuelve a agregarse a vSAN con el nuevo formato en disco.

Nota Una vez que actualice el formato en disco, no podrá revertir el software en los hosts o agregar determinados hosts más antiguos al clúster.

Cuando inicie una actualización del formato en disco, vSAN realizará varias operaciones que puede supervisar desde la página Resincronización de componentes. La tabla resume todos los procesos que se realizan durante la actualización del formato de disco.

Tabla 8-2. Progreso de la actualización

% de finalización	Descripción
0 %-5 %	Comprobación del clúster. Se comprueban y preparan los componentes del clúster para la actualización. Este proceso demora algunos minutos. vSAN comprueba que no existen problemas pendientes que puedan impedir que se complete la actualización. ■ Todos los hosts están conectados. ■ Todos los hosts poseen la versión de software correcta. ■ Todos los discos tienen un estado correcto. ■ Es posible acceder a todos los objetos.
5 %-10 %	Actualización del grupo de discos. vSAN realiza la actualización inicial de los discos sin migración de datos. Este proceso demora algunos minutos.
10 %-15 %	Realineación de objetos. vSAN modifica la distribución de todos los objetos para garantizar que están correctamente alineados. Este proceso puede tardar algunos minutos en un sistema pequeño con pocas instantáneas. Puede demorar varias horas, o incluso días, en un sistema grande con muchas instantáneas, muchas escrituras fragmentadas y varios objetos sin alinear.
15 % - 95 %	Eliminación y reformateo de grupos de discos cuando actualice versiones de vSAN anteriores a la 3.0. Cada grupo de discos se elimina del clúster, se reformatea y se vuelve a agregar al clúster. El tiempo requerido para este proceso puede variar en función de los megabytes asignados y la carga del sistema. La transferencia en un sistema que se encuentra en su capacidad de E/S, o cerca de ella, se realiza lentamente.
95 % - 100 %	Actualización final de la versión de los objetos. Se completa la conversión de los objetos al formato en disco nuevo y la resincronización. El tiempo requerido para este proceso puede variar en función de la cantidad de espacio usado y si está seleccionada la opción **Permitir redundancia reducida**.

Durante la actualización, puede supervisar el proceso de actualización desde la página Resincronización de componentes. Consulte "Supervisar las tareas de resincronización en el clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*. También puede utilizar el comando `vsan.upgrade_status <cluster>` de RVC para supervisar la actualización. Utilice la marca `-r <seconds>` opcional para actualizar el estado de la actualización de forma periódica hasta que presione Ctrl+C. La cantidad mínima de segundos permitida entre cada actualización es 60.

También puede supervisar otras tareas de actualización, como la actualización y la eliminación de dispositivos, en el panel Tareas recientes de la barra de estado.

Al actualizar el formato de disco, se aplican las siguientes consideraciones:

- Si actualiza un clúster con tres hosts y elige la opción **Evacuar todos los datos**, es posible que se generen errores en la evacuación de objetos cuyo **Nivel primario de errores que se toleran** es mayor que 0 (cero). Un clúster con tres hosts no puede reproteger un grupo de discos que está siendo totalmente evacuado con los recursos de solo dos hosts. Es posible que se le solicite agregar otro grupo de discos a un host existente.

  Para un clúster de tres hosts, puede seleccionar la opción de migración de datos **Garantizar disponibilidad**. En este modo, cualquier error de hardware puede producir una pérdida de datos.

  Además, debe asegurarse de disponer de espacio libre suficiente. El espacio debe ser equivalente a la capacidad lógica consumida del grupo de discos más grande. La capacidad debe estar disponible en un grupo de discos independiente del que se va a migrar.

- Cuando se actualiza un clúster con tres hosts o un clúster con recursos limitados, se debe permitir que las máquinas virtuales funcionen en un modo de redundancia reducida. Ejecute el comando de RVC con la opción `vsan.ondisk_upgrade --allow-reduced-redundancy`.

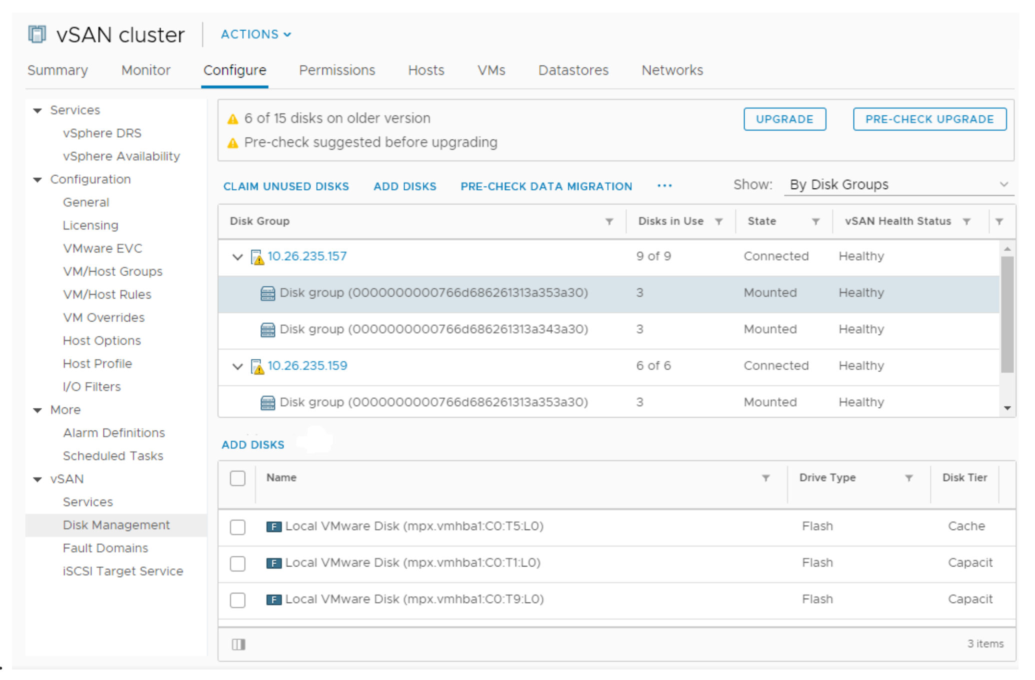
- Si usa la opción de comando `--allow-reduced-redundancy`, es posible que ciertas máquinas virtuales no puedan tolerar errores durante la migración. Esta tolerancia a errores reducida también puede producir pérdida de datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la actualización. Durante la actualización, el estado de cumplimiento de las máquinas virtuales y sus redundancias experimentan un incumplimiento temporal. Una vez que finalizan la actualización y todas las tareas de reconstrucción, las máquinas virtuales pasan a estado de cumplimiento.

- Cuando la actualización se encuentre en progreso, no extraiga ni desconecte ningún host, y no coloque un host en el modo de mantenimiento. Estas acciones podrían provocar errores en la actualización.

Para obtener información sobre los comandos y las opciones de comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Actualizar el formato de disco de vSAN mediante vSphere Client

Una vez que haya terminado de actualizar los hosts de vSAN, puede realizar la actualización del



formato de disco.

Nota Si habilita el cifrado o la desduplicación y la compresión en un clúster de vSAN existente, el formato en disco se actualiza automáticamente a la versión más reciente. Este procedimiento no es obligatorio. Consulte Editar la configuración de vSAN.

Requisitos previos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que esté usando la versión más reciente de los hosts ESXi.
- Compruebe que los discos se encuentren en buen estado. Desplácese hasta la página Administración de discos para comprobar el estado del objeto.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando de RVC, `vsan.whatif_host_failures`, para determinar si dispone de capacidad suficiente para completar correctamente la actualización o recompilar los componentes en caso de que haya errores durante la actualización.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato de disco, no coloque los hosts en el modo de mantenimiento. Cuando un host miembro de un clúster de vSAN entra en modo de mantenimiento, el host miembro deja de aportar capacidad al clúster. Se reduce la capacidad del clúster y se puede producir un error en la actualización del clúster.

- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN. Para obtener información acerca de la resincronización de vSAN, consulte *Supervisión y rendimiento de vSphere*.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Administración de discos**.

4 (Opcional) Haga clic en **Comprobación previa de actualización**.

   La comprobación previa de actualización analizará el clúster para detectar problemas que puedan evitar que la actualización se realice correctamente. Algunos de los elementos que se comprueban son el estado del host, el estado del disco, el estado de la red y el estado de los objetos. Los problemas de actualización se muestran en el cuadro de texto **Estado de comprobación previa de disco**.

5 Haga clic en **Actualizar**.

6 Haga clic en **Sí** en el cuadro de diálogo Actualizar para realizar la actualización del formato en disco.

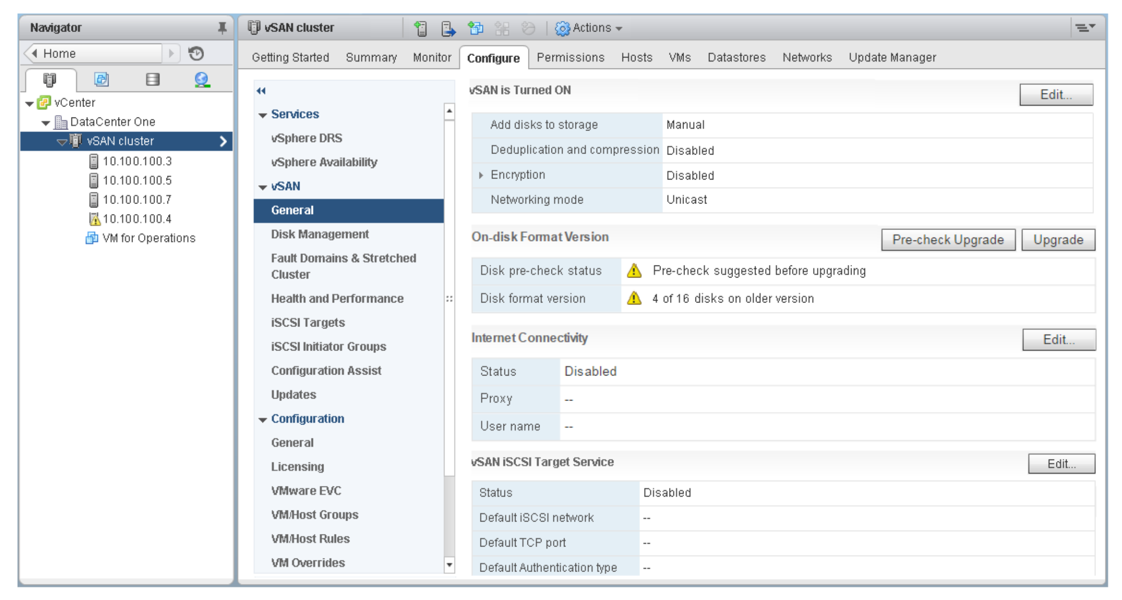
Resultados

vSAN actualiza correctamente el formato en disco. La columna On-disk Format Version (Versión de formato en disco) muestra la versión del formato de disco de los dispositivos de almacenamiento del clúster.

Si ocurre un error durante la actualización, puede comprobar la página Resincronización de componentes. Espere a que se complete la resincronización y vuelva a ejecutar la actualización. También puede comprobar el estado del clúster mediante el servicio de estado. Después de resolver cualquier problema que haya surgido a partir de las comprobaciones de estado, puede volver a ejecutar la actualización.

Actualizar el formato de disco de vSAN mediante vSphere Web Client

Una vez que haya terminado de actualizar los hosts de vSAN, puede realizar la actualización del formato de disco.



Nota Si habilita el cifrado o la desduplicación y la compresión en un clúster de vSAN existente, el formato en disco se actualiza automáticamente a la versión más reciente. Este procedimiento no es obligatorio. Puede evitar reformatear los grupos de discos dos veces. Consulte Editar la configuración de vSAN.

Requisitos previos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que esté usando la versión más reciente de los hosts ESXi.
- Compruebe que los discos se encuentren en buen estado. Desplácese hasta la página Disk Management (Administración de discos) en vSphere Web Client para comprobar el estado del objeto.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando de RVC, `vsan.whatif_host_failures`, para determinar si dispone de capacidad suficiente para completar correctamente la actualización o recompilar los componentes en caso de que haya errores durante la actualización.

- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato de disco, no coloque los hosts en el modo de mantenimiento. Cuando un host miembro de un clúster de vSAN entra en modo de mantenimiento, el host miembro deja de aportar capacidad al clúster. Se reduce la capacidad del clúster y se puede producir un error en la actualización del clúster.
- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN. Consulte "Supervisar las tareas de resincronización en el clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **General**.

4 (Opcional) En **Versión de formato en disco**, haga clic en **Comprobación previa de actualización**.

   La comprobación previa de actualización analizará el clúster para detectar problemas que puedan evitar que la actualización se realice correctamente. Algunos de los elementos que se comprueban son el estado del host, el estado del disco, el estado de la red y el estado de los objetos. Los problemas de actualización se muestran en el cuadro de texto **Estado de comprobación previa de disco**.

5 En **On-disk Format Version** (Versión de formato en disco), haga clic en **Upgrade** (Actualizar).

6 Haga clic en **Sí** en el cuadro de diálogo Actualizar para realizar la actualización del formato en disco.

Resultados

vSAN vuelve a crear cada grupo de discos en el clúster. La columna On-disk Format Version (Versión de formato en disco) muestra la versión del formato de disco de los dispositivos de almacenamiento del clúster. La columna **Disks with outdated version** (Discos con versión desactualizada) indica la cantidad de dispositivos con el nuevo formato. Cuando la actualización se realice correctamente, el valor de **Discos con versión desactualizada** será 0 (cero).

Si ocurre un error durante la actualización, puede consultar la página Resyncing Components (Resincronización de componentes) en vSphere Web Client. Espere a que se complete la resincronización y vuelva a ejecutar la actualización. También puede comprobar el estado del clúster mediante el servicio de estado. Después de resolver cualquier problema que haya surgido a partir de las comprobaciones de estado, puede volver a ejecutar la actualización.

Actualizar el formato de disco de vSAN mediante RVC

Una vez que haya terminado de actualizar los hosts de vSAN, puede usar la herramienta Ruby vSphere Console (RVC) para continuar con la actualización del formato de disco.

Requisitos previos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que la versión de los hosts ESXi que se ejecutan en el clúster de vSAN sea la versión 6.5 o una versión posterior.
- Compruebe que los discos estén en buen estado desde la página Administración de discos. También puede ejecutar el comando de RVC `vsan.disk_stats` para comprobar el estado del disco.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando `vsan.whatif_host_failures` de RVC para determinar si dispone de capacidad suficiente para completar la actualización o realizar una recompilación de componentes en caso de que se produzcan errores durante la actualización.
- Compruebe que PuTTY o un cliente SSH similar estén instalados para acceder a la herramienta RVC.

  Para obtener información detallada sobre la descarga de la herramienta RVC y sobre el uso de comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato en disco, no coloque los hosts en el modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad de recursos disponible se reduce porque el host miembro deja de aportar capacidad al clúster. Es posible que se produzca un error en la actualización del clúster.
- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN mediante la ejecución del comando de RVC `vsan.resync_dashboard`.

Procedimiento

1 Inicie sesión en vCenter Server con la herramienta RVC.

2 Ejecute el siguiente comando de RVC para ver el estado del disco: `vsan.disks_stats /<vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

   Por ejemplo: `vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

   El comando enumera los nombres de todos los dispositivos y los hosts del clúster de vSAN. El comando también muestra el formato de disco actual y su estado de mantenimiento. También puede comprobar el estado actual de los dispositivos de la columna **Estado de mantenimiento** de la página **Administración de discos**. Por ejemplo, el estado del dispositivo que se muestra es Estado incorrecto en la columna **Estado de mantenimiento** para los hosts o los grupos de discos que tienen dispositivos que presentan errores.

3 Ejecute el siguiente comando de RVC: `vsan.ondisk_upgrade <path to vsan cluster>`

Por ejemplo: `vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

4 Supervise el progreso en RVC.

RVC actualiza un grupo de discos a la vez.

Una vez que la actualización del formato de disco finalice correctamente, aparecerá el siguiente mensaje:

```
Finalizó la fase de actualización del formato de disco
```

```
Hay n objetos de v1 que requieren una actualización. Progreso de actualización de objetos:
n actualizados, 0 restantes
```

```
Finalizó la actualización de objetos: n actualizados
```

```
Finalizó la actualización de VSAN
```

5 Ejecute el siguiente comando de RVC para verificar que las versiones de los objetos se actualizaron al nuevo formato en disco: `vsan.obj_status_report`

Comprobar la actualización del formato de disco de vSAN

Una vez finalizada la actualización del formato de disco, debe comprobar si el clúster de vSAN está usando el nuevo formato en disco.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

La versión de formato de disco actual aparece en la parte superior de la página.

Comprobar la actualización del clúster de vSAN

La actualización del clúster de vSAN no finalizará hasta que compruebe que está usando la versión más reciente de vSphere y que vSAN está disponible para su uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configure** (Configurar) y compruebe que aparezca vSAN.

También puede desplazarse hasta el host ESXi y seleccionar **Summary** (Resumen) > **Configuration** (Configuración) y comprobar que utiliza la versión más reciente del host ESXi.

Usar las opciones de comandos de actualización de RVC

El comando `vsan.ondisk_upgrade` proporciona diversas opciones de comando que pueden utilizarse para controlar y administrar la actualización del clúster de vSAN. Por ejemplo, puede permitir una redundancia reducida para realizar la actualización cuando tenga un poco de espacio libre disponible.

Ejecute el comando `vsan.ondisk_upgrade --help` para visualizar la lista de las opciones de comandos de RVC.

Use estas opciones de comandos con el comando `vsan.ondisk_upgrade`.

Tabla 8-3. Opciones de comandos de actualización

Opciones	Descripción
`--hosts_and_clusters`	Use esta opción para especificar rutas de acceso a todos los sistemas host del clúster o los recursos informáticos del clúster.
`--ignore-objects, -i`	Use esta opción para omitir la actualización de un objeto de vSAN. También puede usar esta opción de comando para eliminar la actualización de la versión de un objeto. Cuando use esta opción de comando, los objetos continuarán utilizando la versión de formato en disco actual.
`--allow-reduced-redundancy, -a`	Use esta opción para eliminar la necesidad de contar con espacio libre equivalente a un grupo de discos durante la actualización de discos. Con esta opción, las máquinas virtuales funcionan en modo de redundancia reducida durante la actualización, lo que significa que es posible que ciertas máquinas virtuales no toleren errores temporalmente, y esta incapacidad puede producir pérdida de datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la actualización.
`--force, -f`	Use esta opción para permitir forzar el procedimiento y responder automáticamente todas las preguntas de confirmación.
`--help, -h`	Use esta opción para mostrar las opciones de ayuda.

Para obtener información sobre el uso de los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Recomendaciones de compilación de vSAN para vSphere Update Manager

vSAN genera líneas base del sistema y grupos de líneas base para usarlos con vSphere Update Manager. Puede utilizar estas líneas base recomendadas para actualizar software, revisiones y extensiones de los hosts del clúster de vSAN.

vSAN 6.6.1 y las versiones posteriores generan recomendaciones de compilación automatizadas para los clústeres de vSAN. vSAN combina información de la guía de compatibilidad de VMware y del catálogo de versiones de vSAN con información sobre las versiones de ESXi instaladas. Estas actualizaciones recomendadas proporcionan la mejor versión disponible para asegurarse de que el hardware se mantenga en un estado admitido.

Las líneas base del sistema para vSAN 6.7.1 y versiones posteriores también pueden incluir actualizaciones de firmware y de controladores de dispositivos. Estas actualizaciones admiten el software de ESXi recomendado para el clúster.

En vSAN 6.7.3 y versiones posteriores, puede configurar Update Manager de modo que genere recomendaciones de compilación solo para la versión actual de ESXi o para la versión más reciente de ESXi admitida. Una recomendación de compilación para la versión actual incluye todas las revisiones y las actualizaciones de los controladores correspondientes a la versión.

Líneas base del sistema de vSAN

Las recomendaciones de compilación de vSAN se proporcionan a través de las líneas base del sistema de vSAN para Update Manager. vSAN administra estas líneas base del sistema. Son de solo lectura y no se pueden personalizar.

vSAN genera un grupo de líneas base para cada clúster de vSAN. Las líneas base del sistema de vSAN se enumeran en el panel **Líneas base** de la pestaña Líneas base y grupos. Puede seguir creando y corrigiendo sus propias líneas base.

Las líneas base del sistema de vSAN pueden incluir imágenes ISO personalizadas proporcionadas por proveedores certificados. Si los hosts del clúster de vSAN tienen imágenes ISO personalizadas que son específicas de OEM, las líneas base del sistema recomendadas por vSAN pueden incluir imágenes ISO personalizadas del mismo proveedor. Update Manager no puede generar una recomendación para imágenes ISO personalizadas no admitidas por vSAN. Si ejecuta una imagen de software personalizado que reemplaza el nombre del proveedor en el perfil de imagen del host, Update Manager no puede recomendar una línea base del sistema.

Update Manager examina cada clúster de vSAN de forma automática para comparar el cumplimiento con el grupo de líneas base. Para actualizar el clúster, debe corregir de forma manual la línea base del sistema mediante Update Manager. Es posible corregir la línea base del sistema de vSAN en un único host o en todo el clúster.

Catálogo de versiones de vSAN

El catálogo de versiones de vSAN contiene información sobre las versiones disponibles, el orden de preferencia de las versiones y las revisiones esenciales necesarias para cada versión. El catálogo de versiones de vSAN se hospeda en VMware Cloud.

vSAN requiere conectividad a Internet para acceder al catálogo de versiones. No es necesario que esté inscrito en el Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) para que vSAN pueda acceder al catálogo de versiones.

Si no tiene una conexión a Internet, puede cargar el catálogo de versiones de vSAN directamente en vCenter Server. En vSphere Client, haga clic en **Configurar > vSAN > Actualizar** y en **Cargar desde archivo** en la sección Catálogo de versiones. Puede descargar el catálogo de versiones de vSAN más reciente.

Update Manager le permite importar controladores y firmware de controladora de almacenamiento recomendados para el clúster de vSAN. Algunos proveedores de controladoras de almacenamiento ofrecen una herramienta de administración de software que vSAN puede usar para actualizar el firmware y los controladores de controladoras. Si los hosts ESXi no incluyen la herramienta de administración, es posible descargarla.

Trabajar con las recomendaciones de compilación de vSAN

Update Manager compara las versiones de ESXi instaladas con la información de la lista de compatibilidad de hardware (Hardware Compatibility List, HCL) en la guía de compatibilidad de VMware. Determina la ruta de acceso de actualización correcta para cada clúster de vSAN con base en el catálogo de versiones de vSAN actual. vSAN también incluye las actualizaciones de revisión y los controladores necesarios para la versión recomendada en su línea base del sistema.

Las recomendaciones de compilación de vSAN garantizan que cada clúster de vSAN permanezca en el estado de compatibilidad de hardware actual o superior. Si el hardware en el clúster de vSAN no está incluido en la HCL, vSAN puede recomendar una actualización a la versión más reciente, ya que no es peor que el estado actual.

Nota Update Manager utiliza el servicio de estado de vSAN cuando realiza la comprobación previa de corrección de hosts en un clúster de vSAN. El servicio de estado de vSAN no está disponible en los hosts que ejecutan ESXi 6. 0 Update 1 o una versión anterior. Cuando Update Manager actualiza los hosts que ejecutan ESXi 6.0 Update 1 o una versión anterior, la actualización del último host del clúster de vSAN puede fallar. Si la corrección no se realizó correctamente debido a problemas de estado de vSAN, aún es posible completar la actualización. Utilice el servicio de estado de vSAN para solucionar los problemas de estado en el host y, a continuación, saque al host del modo de mantenimiento para completar el flujo de trabajo de actualización.

Los siguientes ejemplos describen la lógica utilizada por las recomendaciones de compilación de vSAN.

Ejemplo 1

Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. La HCL muestra que el hardware es compatible hasta la versión 6.0 Update 3, pero no para las versiones 6.5 y posteriores. vSAN recomienda una actualización a la versión 6.0 Update 3, incluidas las revisiones esenciales que necesita la versión.

Ejemplo 2

Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. El hardware también se admite en la HCL de la versión 6.7 Update 3. vSAN recomienda una actualización a la versión 6.7 Update 3.

Ejemplo 3

Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware no se encuentra en la HCL de dicha versión. vSAN recomienda una actualización a la versión 6.7 Update 3, a pesar

de que el hardware no aparece en la HCL de la versión 6.7 Update 3. vSAN recomienda la actualización porque el nuevo estado no es peor que el estado actual.

Ejemplo 4

Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. El hardware también es compatible con la HCL para la versión 6.7 Update 3; la preferencia de línea base seleccionada es solo de revisión. vSAN recomienda una actualización a la versión 6.0 Update 3, incluidas las revisiones esenciales que necesita la versión.

El motor de recomendaciones se ejecuta periódicamente (una vez al día) o cuando ocurren los siguientes eventos.

- La pertenencia al clúster cambia. Por ejemplo, cuando se agrega o se quita un host.
- El servicio de administración de vSAN se reinicia.
- Un usuario inicia sesión en My VMware con un explorador web o con RVC.
- Se realiza una actualización en la guía de compatibilidad de VMware o en el catálogo de versiones de vSAN.

La comprobación de estado de la recomendación de compilación de vSAN muestra la compilación actual que se recomienda para el clúster de vSAN. También puede avisarle de cualquier problema existente en la función.

Requisitos del sistema

Update Manager debe instalarse manualmente en vCenter Server de Windows.

vSAN requiere acceso a Internet para actualizar los metadatos de la versión, para comprobar la guía de compatibilidad de VMware y para descargar las imágenes ISO desde My VMware.

vSAN requiere credenciales válidas para descargar desde My VMware imágenes ISO correspondientes a las actualizaciones. En los hosts que ejecutan la versión 6.0 Update 1 o una anterior, debe usar RVC para introducir las credenciales de My VMware. En los hosts que ejecutan software de una versión posterior, puede iniciar sesión desde la comprobación de estado de la recomendación de compilación de ESX.

Para introducir las credenciales de My VMware desde RVC, ejecute el siguiente comando: **vsan.login_iso_depot -u** *<nombre de usuario>* **-p** *<contraseña>*